DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

MCO 3440.8
PS
08 JAN 2008

MARINE CORPS ORDER 3440.8

From: Commandant of the Marine Corps
To: Distribution List

Subj: INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR AND HIGH-YIELD EXPLOSIVE (CBRNE) PROTECTION PROGRAM

Ref: (a) The National Military Strategy of the United States of America, 2004
(b) National Military Strategy to Combat Weapons of Mass Destruction, February 13, 2006
(c) National Response Plan, U.S. Department of Homeland Security, December 2004
(d) DOD Protection Joint Functional Concept, Version 1, June 30, 2004
(e) DOD Instruction 2000.18, “Department of Defense Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines,” December 4, 2002
(f) DOD Instruction 2000.16, “DOD Antiterrorism (AT) Standards,” December 8, 2006
(g) DOD Instruction 6055.06, “DOD Fire and Emergency Services (F&ES) Program,” December 21, 2006
(h) SECNAVINST 3400.4
(i) MCO 3504.2
(j) USMC Installation CBRNE Preparedness Campaign Plan (NOTAL)
(k) MCWP 3-37
(l) SECNAV M-5210.1
(m) Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996,” August 21, 1996

Encl: (1) Installation CBRNE Protection Procedural Guidance

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

1. Situation. Terrorist incidents within the United States and abroad have underscored the Department of Defense's (DOD) need to safeguard military personnel and infrastructure from potential terrorist attacks involving weapons of mass destruction (WMD). While many of the DOD's past efforts have focused on enhancing protection and response capabilities against high explosives, the new security environment underscores the need for the military services to expand its safeguards to include CBRNE events in accordance with references (a) through (m). In order to address these potential threats, enclosure (1) is provided to implement a program for a worldwide USMC installation response capability to mitigate CBRNE events and provide guidance for establishment of an installation CBRNE protection program for emergency responders at USMC installations. At the same time, our Marine Corps Bases (MARCORBASES) will continue to pursue initiatives at their installations to lesson vulnerabilities to terrorist activities.

2. Mission. This Order provides policy and guidance for implementation, execution, and management of the Marine Corps Installation CBRNE Protection Program in support of Marine Corps installation emergency response operations, per references (a) through (m).

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) To define the Marine Corps installations responsibilities in preparation, detecting, assessing, warning, defending and recovering from incidents to include CBRNE warfare and terrorism, accidental and criminal events, and Toxic Industrial Materials (TIMs) releases.

(b) To provide guidance for installations to establish, implement, and maintain a comprehensive preparedness and incident response program capable of addressing CBRNE and TIM incidents with the ultimate objective of protecting personnel, property, and ensuring mission readiness that support the Marine Force (MARFOR) warfighting and the fulfillment of the Commandant of the Marine Corps (CMC) title 10 responsibilities.

(c) This Order does not modify existing military response doctrine, policy, or Tactics Techniques and Procedures (TTPs) related to CBRN Passive Defense but does amplify the preparedness and response requirements associated to the

Installation CBRNE Protection Program as set forth in reference (e).

(d) Prior to and in the event of an incident, installations accomplish the following:

1. Detect. Maintain a high level of situational awareness while detecting, monitoring, and tracking adversary actions and events.

2. Assess (Decide and Task). Conduct analysis of incoming data to define the nature of the threat, and environment.

3. Warn. Use information gained from analysis, provide selective early warning for potential threats, decide on courses of action, and issue appropriate orders and alerts prior to an attack.

4. Defend (Active and Passive). Employ passive and active measures. Passive measures are performed independently and aid in preventing, deterring, delaying, or restricting an adversary. Active protection measures prevent, deter, restrict, resist and/or defeat the threat.

5. Recover. Conduct emergency operations in coordination with tenant organizations, local, county, state, and federal agencies. Effective operations minimize the loss of life and ensure installations continue critical operations that support the warfighting mission during an attack. In addition, restore and resume all other essential operations after an attack.

(2) Concept of Operations (CONOPS)

(a) Consistent with the policy to coordinate and integrate multiple programs that operate with similar and/or overlapping requirements, installation CBRNE protection CONOPS incorporate and address planning and implementation, which are divided into three operational phases: Pre-Incident, Incident Response, and Post-Incident. The three phases are sustained in a continuous cycle and are supported by the following activities:

1. Baseline program determinations and assumptions.

2. Implementation of an Installation CBRNE Protection Working Group.

3. Installation and regional threat assessments.

4. Integrated vulnerability assessments.

5. Risk assessment and analysis.

6. Identification of organic baseline emergency response and civil support capabilities.

7. Active/passive CBRNE preparedness, defense, and response measures.

8. Training, education, and exercises.

9. Logistics and administration.

(b) The installation CBRNE protection CONOPS includes strategic coordination and integration of CBRNE policy and program level activities. The Deputy Commandant (DC), PP&O has overall responsibility for installation CBRNE Protection policy and coordination within the Marine Corps. The DC, PP&O synchronizes efforts between policy development, maintenance and sustainment of installations, specific requirement generation & validation, operational testing, and systems acquisition related to installation CBRNE protection.

(c) Commanders MARCORBASES (COMMARCORBASES), Commanding Generals of Marine Corps Installations (MCIs), and Commanding Generals and Commanding Officers of non-regionalized installations employ appropriate resources such as, personnel, forces, equipment, supplies, and facilities under their cognizance in responding to CBRNE incidents and emergencies. On order, provide support to civil authorities during emergencies.

(d) Align CBRNE incident plans with and integrate into existing Force Protection (FP), Antiterrorism (AT), Critical Infrastructure Protection (CIP), and Emergency Security Systems (ESS) plans.

(e) Maintain an emergency response capability. This capability is not valid until it is properly organized, equipped, trained, exercised, and sustained. Capability level is determined solely by the unique requirements,

characteristics, and circumstances of each installation, to include:

1. Installation mission. Installations provide the enablers for deployment of Marine Forces to enhance their ability to project forces in support of combatant command requirements. Installations enhance and enable the ability of the Commandant in fulfilling his title 10 responsibilities to train, organize, and equip Marine Forces in support of combatant command requirements.

2. Protection of critical mission assets and infrastructures in varying hazardous environments.

3. Maintaining essential operations and support of personnel.

4. Availability of community emergency response support adjacent to Marine Corps installations. Such support does not negate the requirement for each installation to develop and maintain an organic emergency response capability.

5. Characteristics and population density of each installation.

b. Subordinate Element Missions. Commandant of the Marine Corps (CMC) executes the coordination of installation CBRNE protection policy through the appointment of the following:

(1) Deputy Commandant, Plans, Policy and Operations (DC, PP&O):

(a) Overall responsibility for the development, implementation, and execution of installation CBRNE protection policy within the Marine Corps.

(b) Focal point and advocate for installation CBRNE protection policy, integration, and coordination issues within the Marine Corps and coordination of such activities within the Department of the Navy.

(c) Represent the Marine Corps in Joint DoD efforts pertaining to the standardization and uniform application of various components of installation CBRNE protection requirements and programs.

(d) Designate a centralized program manager for Marine Corps first responders and installation CBRNE protection strategy, policy, and program capabilities development.

(e) Provide representation for the development of Combating Weapons of Mass Destruction (CBT WMD) policy and capabilities.

(f) Serve as the liaison between HQMC, COMMARCORBASES, Marine Corps Installations, and non-regionalized installations. Initiate, develop, and implement uniform methodologies, processes, and procedures for installation CBRNE education, training, and exercises to be implemented at the MARCORBASES level.

(g) Program resources to support the design of training and exercises in order to test at a minimum both military and civilian activities normally associated with the initial responses to an installation CBRNE mass casualty incident.

(h) Develop a centralized data collection system for installation CBRNE related programs, initiatives, points of contacts, and funding requirements.

(i) Coordinate and integrate detection, warning, and decision support system technologies and capabilities. Integrate these capabilities into a single system providing a real-time common operating picture for Anti-terrorism/Force Protection (AT/FP) postures, CBRNE threat monitoring and detection, automated warning and reporting, and decision support system.

(j) Provide guidance for the Marine Corps CBRNE Installation Protection Program (IPP) and first responders. Review the feasibility of extending the sensor and monitoring networks from installations to vital deployment routes and staging areas for power projection.

(k) Identify the requirements, capabilities, and program resources to sustain future maintenance, training, and personnel support for CBRNE monitoring and detection programs for the installation CBRNE protection and first responders.

(l) In coordination with Deputy Commandant, I&L and Deputy Commandant, C4 determine if certain portions of Marine Corps installations be provided collective protection, such as

in critical C4I areas, Emergency Operation Centers (EOCs), and other mission critical assets to support continuation of critical operations in a CBRNE environment.

(2) Deputy Commandant for Installations and Logistics (DC, I&L):

(a) In coordination with Deputy Commandant, PP&O and Deputy Commandant, C4, jointly operate as integral partners to define, develop, and implement appropriate installation CBRNE preparedness and response capabilities.

(b) In coordination with DC, PP&O, determine if certain portions of installations be collectively protected (i.e. critical C2 areas or nodes), IOT support continuation of critical operations in a hazardous environment.

(c) Analyze and provide support for critical infrastructure protection of critical maintenance, supply, and logistics processes, facilities, and assets against CBRNE.

(d) Address public works requirements for WMD incidents. This includes pre-incident requirements, estimated power and water requirements supporting on-site decontamination, procedures to control decontamination run-off, and operational procedures for providing back-up power on-site, removing debris, and deploying incident response and damage assessment teams.

(e) Address mass care planning, such as sheltering, feeding, quarantine/sequestering or otherwise caring for victims or evacuees following a CBRNE incident.

(3) Deputy Commandant, Combat Development and Integration (DC, CD&I):

(a) In coordination with DC, PP&O, develop, integrate, and validate capabilities for installation CBRNE protection and first responder requirements.

(b) In coordination with DC, PP&O, develop doctrine for installation CBRNE protection within and outside the United States.

(c) Identify and provide the resident Chemical, Biological, Radiological, and Nuclear (CBRN) expertise required to assist in the development of installation CBRNE protection training and education curricula.

(d) Define and implement training programs at Military Occupational Specialty (MOS) schools to meet the requirements for operations and maintenance of advanced CBRNE protection technologies that support the CBRNE Installation Protection Program.

(e) Include both military and civilian personnel supporting installation CBRNE protection and first responders in training initiatives to including senior leadership training and orientations.

(f) Develop additional training for CBRN MOS billets that focus on providing knowledge of installation CBRNE protection, FP, AT, vulnerability analysis, Hazardous material (HAZMAT), National Incident Management System (NIMS), National Response Plan (NRP), Emergency Operations Center (EOC) operations, and commercial-off-the-shelf (COTS) hazard prediction systems.

(4) Director, Marine Corps Operational Test and Evaluation Activity (MCOTEA):

(a) Develop and incorporate realistic operational scenarios and mission tasks into Part IV of Test and Evaluation Master Plans (TEMPs). Participate as a charter member in the material developer designated and chaired Test and Evaluation Working Integrated Product Teams (T&E WIPTs) in support of the installation CBRNE material acquisition programs.

(b) Evaluate Information Assurance (IA) protection, detection, reaction, and response mechanisms as a function of Mission Assurance Category (MAC) during operational test and evaluation.

(c) Evaluate the impact of security certification and accreditation, joint interoperability, electromagnetic environmental effects, and spectrum management as requirements of installation CBRNE protection planning.

(5) The Inspector General of the Marine Corps (IGMC):

(a) Coordinate with the DC, PP&O (Security Division (PS)) regarding integration of the provisions of this order into the Automated Inspection Reporting System (AIRS) checklist.

(b) Conduct reviews as part of the Marine Corps Command Inspection Programs to determine compliance with the requirements contained herein.

(c) Develop policy guidance and best practices with respect to planning, developing, and executing military-civilian mutual aid agreements.

(6) Director, Health Services:

(a) Coordinate with Bureau of Medicine and Surgery (BUMED) ensuring every installation Medical Treatment Facility (MTF) develops installation CBRNE protection procedures, including the provision of pre-hospitalization emergency response capabilities such as triage, treatment, and transport. This coordination includes:

1. Protocols and guidelines for initiating medical surveillance. Establish routine monitoring prior to the occurrence of a crisis.

2. Treatment protocols for medical diagnosis and treatment in a contaminated environment, to include when to medicate, when to clean, and when to stop treatment to avoid further loss through cross-contamination or spread of chemical and biological agents are examples.

3. Identify the effectiveness of various medications in treating the effects of chemical and biological agents.

4. Publish priority treatment protocols for essential personnel, both military and civilian, necessary to maintain critical functions and missions during a CBRNE event.

5. Develop emergency treatment protocols for dependents, civilian contractors, and host nation workers.

6. Develop programs emphasizing pre-incident treatment efforts, such as inoculations, rather than relying on less effective post-incident treatments.

7. Address latent or chronic health issues that arise from exposure to CBRNE hazards by working with appropriate state and federal agencies.

8. Identify State and Local assets that could provide assistance. Identify and procure appropriate medical

stockpiles and evacuation assets. Establish procedures to manage supply routes and/or medical materiel distribution during an incident.

9. In coordination with the Staff Judge Advocate to the Commandant of the Marine Corps (SJA to CMC), define policy and set forth legal guidelines with regard to sharing medical information for governmental purposes, including medical surveillance IAW reference (m).

10. Identify procedures for the safe care and handling of the contaminated remains of our personnel who have fallen victims to CBRNE events.

11. Address collective protection requirements for triage or medical/surgical treatment facilities.

(7) Commander, Marine Corps Systems Command (MCSC):

(a) Provide USMC representation to future Joint Program Executive Office, Chemical and Biological Defense Program (JPEO CBD) Integrated Product Teams (IPTs).

(b) Ensure USMC interoperability and standardized requirements are met.

(c) Ensure the equipment selection complements the technologies of civilian first responders and emergency responders which support the installation CBRNE protection program.

(8) SJA to CMC:

(a) Provide legal support to DC, PP&O, in the development, implementation, and execution of installation CBRNE protection policy.

(b) Provide guidance related to the development and implementation of joint mutual aid and assistance agreements for joint military-civilian emergency response activities.

(c) In coordination with Health Services, define policy and set forth legal guidelines with regard to sharing medical information for governmental purposes, including medical surveillance IAW reference (m).

(d) In coordination with Health Services, review and refine policy and guidance regarding:

1. The nature and scope of authority to impose quarantine during a CBRNE incident, pandemics or other catastrophic event.

2. Rules regarding the use of force during varying medical quarantine scenarios.

3. How, and to what extent, the military should assist civilian authorities in supporting a quarantine scenario outside the installation perimeter.

(9) Deputy Commandant for Programs and Resource (DC, P&R):

(a) Actively advocate for installation CBRNE protection funding and resources by establishing direct liaison with Deputy Commandant, PP&O, PS Division, Deputy Commandant, I&L, and Deputy Commandant, C4 to coordinate and identify near-, mid- and long-term funding requirements and funding sources.

c. Command Responsibilities

(1) Commanders MARCORBASES (COMMARCORBASES):

(a) Develop and provide guidance and standards to assist installations to establish installation CBRNE protection plans.

(b) Establish regional CBRNE planning and response procedures to oversee and provide for mission continuity and the safety and well-being of assigned military personnel, families, and civilian employees during CBRNE events.

(c) Provide oversight and assessment of installation CBRNE protection plans to ensure these programs and plans effectively meet regional installation requirements.

(d) Prepare regional CBRNE plans that specify actions required for rapid response, mitigation, efficient use of resources within the Area of Responsibility (AOR), and transition to recovery. As part of the regional planning effort, identify critical mission assets and infrastructures on installations that must be protected and sustained in varying hazardous environments.

(e) Overseas commanders coordinate installation CBRNE protection planning with the Department of State (DOS) via theater combatant commanders and assigned embassies and/or consulates.

(f) Provide guidance on resource requirements and priorities to installation commanders. Validate and prioritize subordinate installation CBRNE protection resource requirements.

(g) Provide intelligence information, threat assessments, and warnings to installations within the MARFOR geographic region.

(h) Provide military support/ assistance to local civil authorities as directed.

(i) Maintain all records concerning development of CBRNE plans per reference (l) SSIC 3000.5a.

(2) Marine Corps Installation Commanders:

(a) Prepare, implement, maintain, and exercise an installation CBRNE protection plan to manage the consequences of a CBRNE incident in order to:

1. Enhance safety, protect life, health and the environment.

2. Protect critical assets and infrastructures vital to mission execution.

3. Ensure continued operation of mission critical/essential functions during a CBRNE incident.

(b) Develop an installation CBRNE protection plan that specifies action required for rapid incident response, mitigation, efficient use of resources, and transition to recovery operations.

(c) Identify required resources to establish, maintain, and execute an installation CBRNE protection plan with activities consistent with missions supported; critical assets/infrastructures supporting mission execution; and threat, vulnerability, and risk assessments.

(d) Develop, implement, and maintain the capability to facilitate recovery operations to re-establish all other installations operations and functions after a CBRNE incident.

(e) Establish Mutual Aid Agreements (MAAs) or Memoranda of Understanding/Agreement (MOUs/MOAs) with local, state, federal, and/or host nation incident response and/or emergency management organizations pursuant to all applicable DOD rules, regulations, and policies.

(f) Establish an emergency management and response organization to provide for mission continuity, to ensure the well-being of assigned military personnel, families, and civilian employees during CBRNE events, and to enhance safety to protect life, health, and the environment.

(g) Include tenant commands, deployable units, and applicable local, state, federal, and/or host nation agencies in the CBRNE organization and plan.

(h) Assign and designate CBRNE protection officers based on installation physical infrastructure, mission, and available personnel including tenant command, active, and Reserve personnel.

(i) Overseas installation commanders, in addition to the stated Installation Commander responsibilities, shall:

1. Support combatant commander requirements as vetted through appropriate MARFOR chain of command.

2. Integrate installation capabilities with host nation capabilities to the degree needed to ensure availability of recovery capabilities and continuance of the installation mission.

3. Establish MAAs with host nation emergency response agencies for mutual support pursuant to all applicable DOD rules, regulations, and policies.

4. Support Non-Combatant Evacuation Operations (NEO) in the event of an emergency precipitated by a CBRNE incident.

(j) Integrate Explosive Ordnance Disposal (EOD) into installation CBRNE protection plans.

(k) Integrate and coordinate protection and response activities into a protection working group that provides support to installation CBRNE protection planning.

(l) Ensure assigned personnel are appropriately organized, trained, equipped, and sustained to provide emergency response to all applicable hazards and CBRNE threats. Ensure first responder teams receive initial and follow-on training required for performance of assigned responsibilities.

(m) Formally assess installation vulnerability on an annual basis.

(n) Coordinate receiving and evaluating national intelligence and higher headquarters threat assessments and warnings to determine their applicability. In conjunction with Naval Criminal Investigative Service (NCIS), prepare and maintain a local threat assessment that is specific to the installation's mission, assets, and geographic location.

(o) Provide basic CBRNE awareness training on protective measures to the installation population in conjunction with AT Level I training. Ensure installation personnel are aware of the mitigation and response actions such as mass notification and shelter-in-place (SIP) to be undertaken in the event of CBRNE warfare, terrorism, accident, or incident.

(p) Identify training requirements, and include those requirements in the budget process for funding. Tailor training to meet the specific circumstances of the installation.

(q) Establish an exercise and evaluation program to validate the installation CBRNE protection CONOPS. Conduct one CBRNE field training exercise annually that:

1. Assesses and evaluates, at a minimum, first responders, incident command, and the emergency operations center. Annual AT plan exercises will be combined with CBRNE field training exercises as directed by reference (f) and maintained per reference (l) SSIC 1510.3 for enlisted personnel, SSIC 1520.1 for Officers and SSIC 12410.14 for civilian personnel.

2. Validates the full capability of the integrated installation response organization to respond to CBRNE incidents and evaluate the ability to preserve critical military functions and restore essential operations.

(r) Provide OPREP-3SIR (Serious Incident Report) reports to the Commandant of the Marine Corps through the Marine Corps Operations Center (MCOC), with information on significant

CBRNE events or incidents in accordance with reference (i) and maintained per reference (l) SSIC 3005.5b.

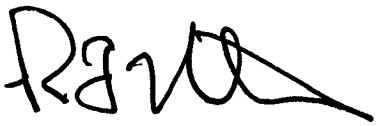
(s) Maintain all records concerning development of CBRNE plans per reference (l) SSIC 3000.5a.

4. Administration and Logistics. Recommendations concerning the contents of this Order may be forwarded to DC, PP&O (PS) via the appropriate chain-of-command.

5. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force.

b. Signal. This Order is effective the date signed.



R. F. NATONSKI
Deputy Commandant for
Plans, Policies and Operations

DISTRIBUTION: PCN 10203060300

LOCATOR SHEET

Subj: INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR AND HIGH-YIELD EXPLOSIVES (CBRNE) PROTECTION PROGRAM

Location: _____

(Indicate the location(s) of the copy(ies) of this Order.)

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

TABLE OF CONTENTS

Chapter 1

EMERGENCY RESPONSE GUIDELINES

1. Purpose

a. Implement policy, assign responsibilities, and provide procedural guidance to establish and implement a Marine Corps installation Chemical, Biological, Radiological, Nuclear or High-Yield Explosive (CBRNE) protection program for a worldwide installation emergency response to manage the consequences of CBRNE incidents.

b. Provide guidance for the establishment of an installation CBRNE protection program for emergency responders at Marine Corps installations. Marine Corps installation emergency responders must prepare to respond to the effects of a CBRNE incident to preserve life, prevent human suffering, mitigate the incident and protect critical assets and infrastructure. An overview of the installation CBRNE protection program is provided below in Figure 1-1.

Figure 1-1.--Installation CBRNE Protection Program Overview

2. Policy. In accordance with the references of this Order it is policy that:

a. The DOD Components in the Continental United States (CONUS) have the responsibility, as specified in U.S. law, to support and assist U.S. civil authorities, as directed, in consequence management activities for natural and man-made disasters to include CBRNE related events on U.S. territory and abroad. An overview of this approach and the demographics are depicted in Figure 1-2.

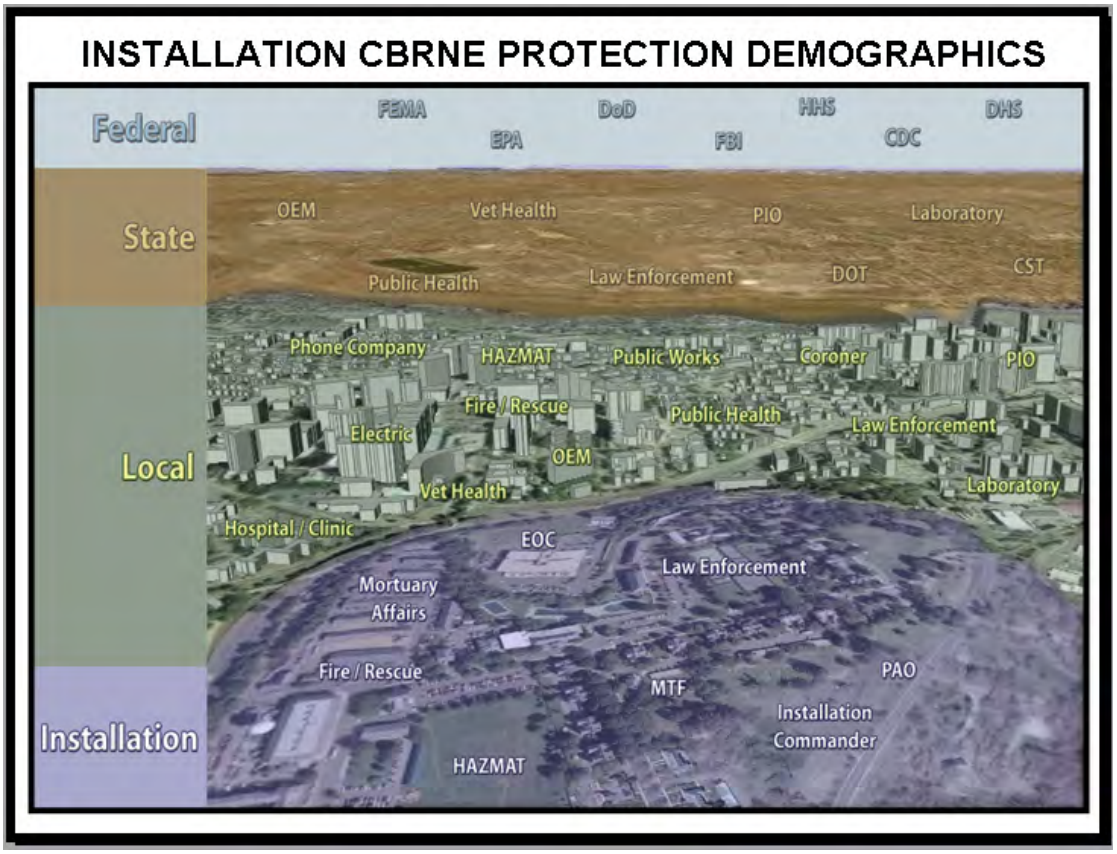


Figure 1-2.--Installation CBRNE Protection Demographics Overview

b. Commanders implement multi-layered approaches of active and passive deterrence, including dedicating resources to Consequence Management (CM). An overview of this approach is depicted in Figure 1-3.

(1) Commanders are prepared to respond to and protect DOD personnel and installations from the effects of a CBRNE incident.

(2) Commanders at all levels have the authority and responsibility to protect persons and property subject to their control.

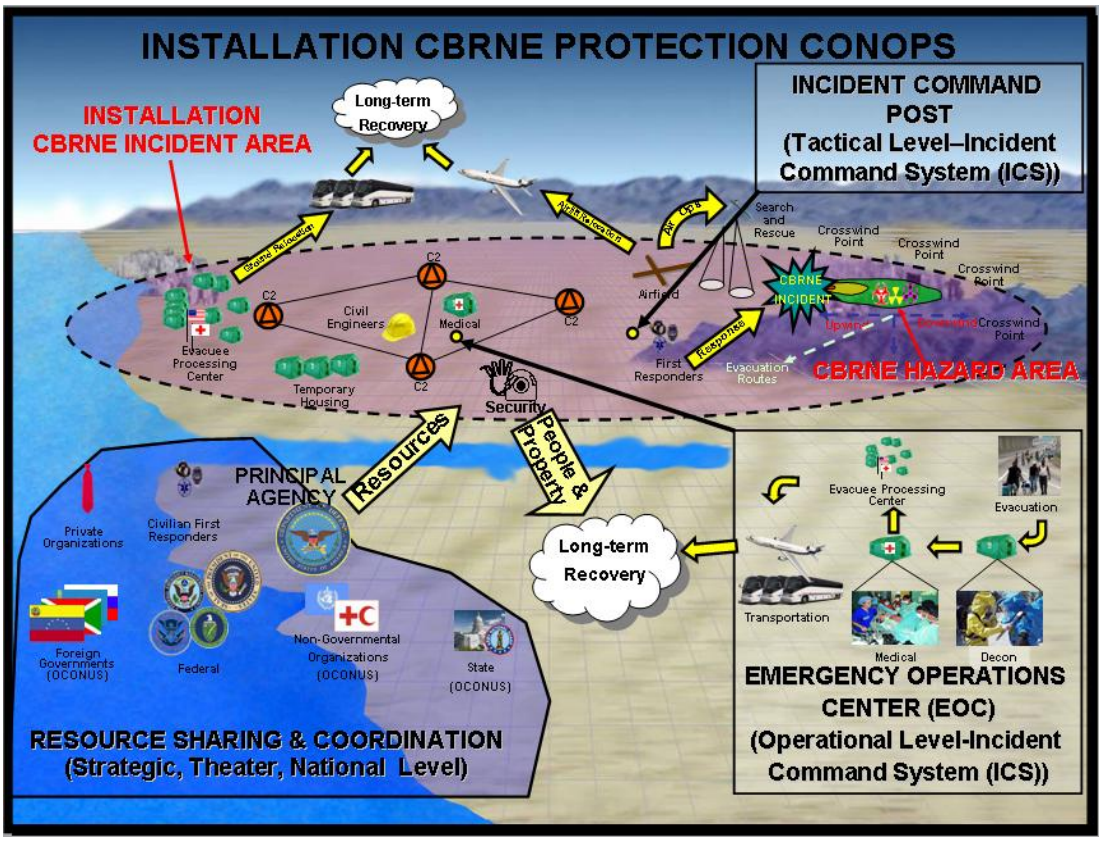


Figure 1-3.--Multi-layered Approach Installation CBRNE Protection

c. Nothing in these guidelines should be interpreted to subsume, replace, detract from, or conflict with, authorities and responsibilities of commanders specified by law or DOD guidance.

3. Responsibilities. COMMARCORBASES in the Continental United States (CONUS) and outside the Continental United States (OCONUS) shall:

a. Ensure compliance with the guidelines provided in references (e) and SECNAVINST 3400.4 and this Order.

b. Institute an installation monitoring process to:

(1) Ensure installations schedule and conduct emergency response exercises involving and measuring emergency response capabilities to CBRNE incidents.

(2) Review recommended type and frequency of installation CBRNE protection exercises delineated in local installation Integrated Vulnerability Assessments.

c. As appropriate, support emergency response initiatives for installation CBRNE protection with adequate and appropriate programming, planning, personnel, training, exercises, and funding.

d. Ensure installation CBRNE protection emergency response policies, plans, procedures and guidelines are supported by sufficient command and control capabilities and other equipment to properly respond to CBRNE incidents.

e. Institute emergency response programs for CBRNE on installations to include Active and Reserve component installations, Reserve centers and armories, as appropriate, in CONUS.

f. Incorporate lessons learned from installation emergency response CBRNE exercises into existing overall installation force protection plans.

g. As appropriate, establish or facilitate formal training programs that provide installation emergency response planners and emergency responders instruction in planning and response for CBRNE incidents.

4. Installation Commanders Guidelines

a. Guideline 1: Implementation and Oversight

(1) Commanders are responsible for the implementation of DOD Installation CBRNE emergency response policies within their organizations.

(2) Commanders shall develop and implement a comprehensive CBRNE emergency response program at installations under their control to comply with the guidelines contained in this Order.

(3) Commanders shall develop base-wide or regional scenarios designed to establish baseline capabilities needed to

allow installation emergency responders to protect personnel and infrastructure, facilities, other assets, and identify vulnerabilities.

(4) Commanders shall use guidelines contained herein as baseline guidelines.

(5) Commanders may promulgate unique requirements in their implementing directives to supplement the standards contained herein. As a minimum, these guidelines should address the following areas:

(a) Develop, train, exercise, maintain, sustain, and assess procedures that shall promote the preparation for responding to and mitigating the effects of a CBRNE event on installations.

(b) Develop, maintain, and sustain CBRNE emergency response plans and procedures to enhance installation emergency response capabilities.

(c) Conduct vulnerability assessments for CBRNE response preparedness and identify critical infrastructure nodes that can affect an installation's or tenant organization's ability to perform its mission.

(d) Establish CBRNE emergency response procedures and identify CBRNE emergency response requirements. Include program resources necessary to meet installation CBRNE emergency response needs and comply with appropriate DOD Instructions.

(e) Develop, maintain, and execute CBRNE emergency response measures to include detection, assessment, response capabilities, medical treatment, containment, emergency responder casualty decontamination, and reporting.

(f) Commanders should prepare emergency response support measures to address CBRNE incidents on U.S. installations overseas. Commanders should become familiar with any Status of Forces Agreements (SOFAs) and other international agreements affecting CBRNE response as well as host-nation emergency response capabilities appropriate to the installation.

(g) CBRNE Emergency Responder Program Criteria. DOD installations, regardless of size, should have some basic level of CBRNE emergency response capability and support. This capability could be organic or provided by local or host-nation

agencies. The following defines an installation responsible for the establishment of a CBRNE emergency response program:

1. DOD installations.

2. Installations that have assigned Federal emergency response personnel and capabilities dedicated to emergency response functions for the installation.

(h) Commanders should consider the following categories when determining priority for the allocation of limited resources for the development of installation CBRNE emergency response capabilities:

1. Installations and/or facilities critical to overall accomplishment of the National Military Strategy (NMS). This includes installations that contain one-of-a-kind strategic assets, major troop concentrations, strategic lift assets, command, control, communications, and intelligence (C3I) critical assets and infrastructure, major ports of embarkation and debarkation, key logistic sites, mobilization sites, and those installations that support national strategic objectives essential to national security during times of war and national emergencies.

2. Non-power projection installations/ facilities that provide combat service support, such as supply depots, logistics centers, and other installations but are still assigned a mission directly related to accomplishment of the NMS.

3. Installations or facilities. This may include installations that provide or include research and development, acquisition, testing and evaluation, production, training, and administration.

b. Guideline 2: Management Responsibilities

(1) Commanders are responsible for establishing a CBRNE emergency response program on the installation. A well-designed CBRNE emergency response program shall be implemented to provide long-term direction by guiding the installation emergency responders in a coordinated series of steps. In some locations, an area commander having responsibility for multiple installations within close proximity may develop a CBRNE program on an area vice installation level. Where this is applicable, other guidelines contained in this Order may also be developed

and executed on an area basis, as appropriate. Commanders shall:

(a) Develop a CBRNE emergency response plan that integrates facilities, equipment, training, personnel, and procedures into a comprehensive effort designed to provide appropriate protection to personnel and critical mission on the installation.

(b) Identify responsibilities, resources, and requirements for successful execution of CBRNE emergency response plan.

(c) Supervise, assess, exercise, and review the CBRNE emergency response program capabilities on the installation.

(d) Designate a commissioned officer, non-commissioned officer, or civilian staff officer in writing as the installation CBRNE protection officer with CBRNE emergency response program management responsibilities.

(e) Assign the installation CBRNE protection officer the responsibilities for development, coordination, and management of the installation CBRNE emergency response plan. The CBRNE emergency response plan will be developed as an annex to the existing AT plan or as a stand alone document.

(d) Create an installation CBRNE emergency response-working group within the Installation Force Protection Committee to be responsible for planning, assessing, training, and exercising the installation CBRNE program.

(2) The CBRNE Emergency Response Working Group should:

(a) Provide a forum for commanders to execute directions and decisions on issues related to CBRNE emergency response.

(b) Invite and include liaison personnel from appropriate local/state/federal/host-nation emergency response management responder communities and tenant organizations, as necessary. Evaluate and modify existing MAAs/MOUs when and where appropriate.

(c) Integrate installation CBRNE emergency response initiatives into installation resource planning.

(d) Collect and prioritize installation CBRNE emergency response resource requirements for the Program Objective Memorandum (POM) submission. As appropriate, chemical, biological, and radiological procurements requirements should be submitted through the DOD Chemical, Biological Defense Program budget process. All other requirements should be submitted through the Marine Corps budget process.

(e) Ensure that the installation's CBRNE emergency response plan is integrated with local emergency response plans, as necessary.

(f) Ensure the installation develops plans and conducts appropriate training for CBRNE Emergency Response teams and personnel.

(g) Conduct assessments regarding the current status of the installation's capabilities to include strengths and weaknesses of the CBRNE emergency response program.

(h) Conduct and maintain an annual vulnerability analysis and risk assessment to determine installation shortfalls and vulnerabilities to CBRNE attacks.

(i) Coordinate meetings, as necessary, with emergency responders on and off the installation.

(j) Ensure all CBRNE plans are maintained per reference (l) SSIC 3000.5a.

(3) In addition to paragraph 6.b.1, Overseas Installation Commanders shall:

(a) Assess the capability of the installation's emergency responders to conduct a baseline assessment of the installation's CBRNE response capabilities and measure the ability of the host nation's emergency response capabilities to support the installation. This assessment should include a review of personnel, equipment, training, and exercises. In those cases in which the installation is completely dependent upon host-nation assets, commanders shall work with the host-nation responders and jointly conduct this assessment.

(b) Integrate installation emergency response capabilities with host-nation emergency responders to the degree needed to ensure the availability of proper response, casualty decontamination, mitigation capabilities, and continuance of

the installation mission.

(c) Include in the installation CBRNE emergency response plan measures that address security and/or possible evacuation of DOD personnel and their dependents.

(d) Become familiar with SOFAs and other international agreements affecting CBRNE response as well as host-nation emergency response capabilities appropriate to the installation.

(e) Coordinate CBRNE emergency response efforts on the installation internally and engage with local host-nation emergency responders or their representatives to ensure interoperability.

(f) Implement existing memorandums of understanding (MOUs) and/or memorandums of Agreement (MOAs) with host nations, as necessary, to ensure host-nation CBRNE emergency response capabilities are integrated into installation CBRNE protection/response plans. With proper authority and approval, negotiate and complete such MOUs/MOAs where they do not exist.

(g) Review MOUs and/or MOAs annually to ensure that host-nation sufficiency exists in meeting agreed upon installation emergency response needs.

(h) Develop appropriate scenarios for CBRNE exercises that integrate host nation and installation CBRNE emergency response capabilities.

(i) Seek and leverage training opportunities to include integration of planning, training, and exercises involving any Combatant Commander's CBRNE emergency response elements.

c. Guideline 3: Functions

(1) CBRNE emergency response functions include preparedness, response, and recovery operations. Requisite staff functions include health and medical services, public affairs, legal counsel, public works and safety, chaplain services, mortuary affairs, and resource management. Each response function shall be integrated into a CBRNE emergency response Concept of Operations (articulating who, what, with what, how, where, when) at each installation.

(2) Command, control, and communications management should include the establishment of an installation Incident Command System (ICS) and an Emergency Operations Center (EOC) and, when warranted, an alternate EOC. The EOC should have a well-defined communications plan that may include the capability to communicate with civil authorities and standard operating procedures for monitoring incident development. The installation ICS is depicted in Figure 1-4 below:

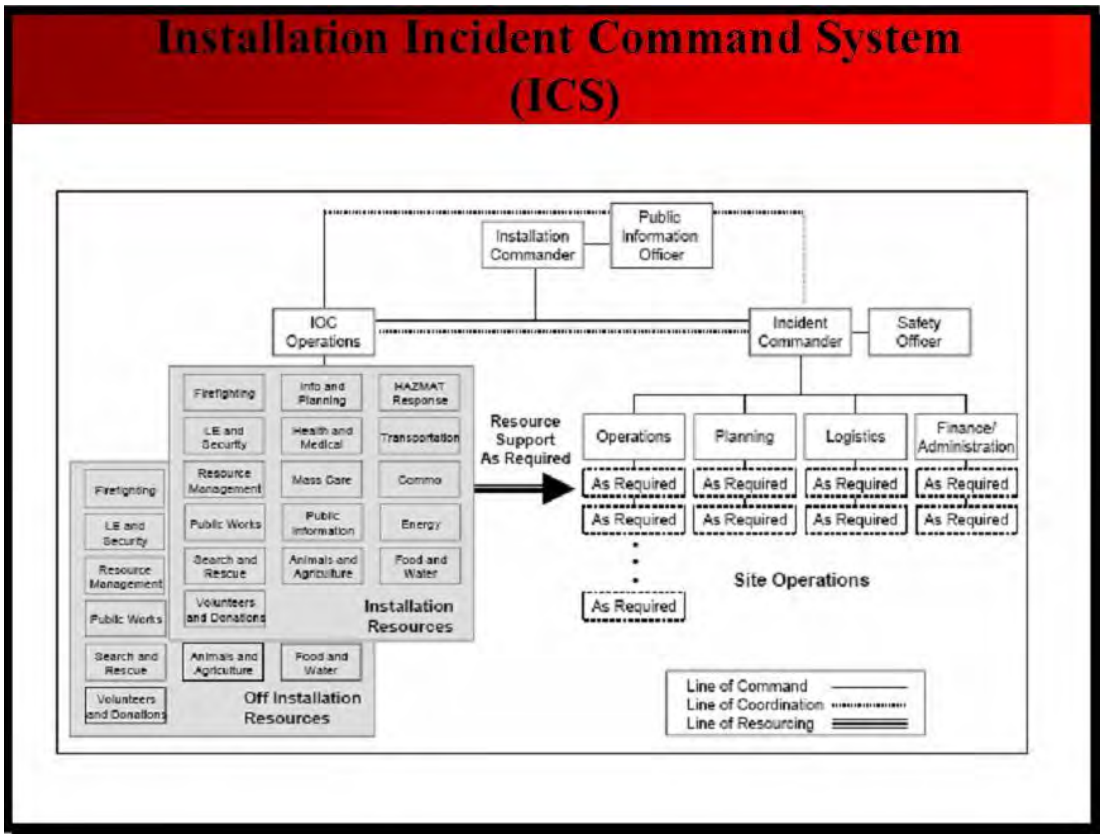


Figure 1-4.--Installation Incident Command System (ICS)

(3) Law enforcement and/or security response functions to CBRNE events should include securing an appropriate perimeter around the CBRNE incident, establishment of entry and/or exit control procedures, establishment of traffic control points, chain of custody rules, assessment and/or detection, evidence preservation and chain of custody procedures, and maintenance of installation security. Searches for secondary devices should be done in conjunction with EOD team members.

(4) Fire and hazardous material response functions to CBRNE events should include: establishing command, control,

communications, accountability; fire suppression, rescue, extrication; atmospheric monitoring and detection; environmental sampling to determine contaminant and level of contamination; triage; mass decontamination of ambulatory and non-ambulatory patients; and preserving evidence. Specific fire and/or hazardous material (HAZMAT) response core functions include the following:

(a) Atmospheric monitoring and detection needed to determine the level and extent of chemical, biological, and radiological contamination. This guideline requires portable detection devices, a communications capability to the central emergency operations center, as well as individual protective equipment. If further confirmation is required, an approved and designated laboratory should be used for authoritative and verifiable analysis.

(b) Extract casualties from a CBRNE environment. This guideline requires individual protective equipment and individual communications capability to a central emergency operations center with the capability to transport a casualty out of a contaminated area.

(c) Decontaminate and treat chemical, biological, or radiological contaminated casualties. This guideline requires a capability to provide needed medical care during the decontamination process, with individual protective equipment and communications capability to a central emergency operations center for the purposes of decontaminating a contaminated casualty and stabilizing casualties for evacuation to higher-level medical care.

(5) Health and medical response functions should include emergency casualty decontamination at medical treatment facilities and include mass casualty triage, treatment, quarantine, transport, psychological casualties, supplies, pharmaceuticals and vaccines, alternate treatment facilities, mass casualty care, and restriction of movement procedures. Specific health and medical response core functions include the following:

(a) Medical surveillance for illness resulting from exposure to a biological agent. This guideline addresses the ability to maintain surveillance for the outbreak of illness resulting from the exposure to a biological agent. Surveillance may include monitoring and analysis of clinical trends or

pharmaceutical use, and sampling for biological agents. At a minimum, this surveillance should be able to identify that an outbreak of illness is occurring early enough in time to potentially mitigate significant adverse impact of the disease on the mission of the installation. A capability and expertise to identify an unknown biological agent or the capability to quickly contact an organization qualified to do so must be maintained.

(b) Medical management of illness resulting from exposure to a biological agent. This guideline addresses maintaining the medical capability to identify an unknown biological agent causing an outbreak of illness and to medically respond with prophylaxis and/or treatment to mitigate significant impact of the disease on the mission of the installation or to have the capacity to meet this requirement through a supporting organization.

(6) EOD operations include the detection, identification, analysis, render-safe, recovery, and disposal of primary and secondary devices. The closest EOD team and/or unit shall provide site-stabilizing initial support, and assist responding national assets and EOD teams upon their arrival. While preservation of evidence is highly desirable, actions to recover and/or preserve evidence shall not compromise the safety of any personnel.

(7) Installation procedures regarding mortuary affairs response functions should include fatality management and contaminated casualty and/or remains handling.

d. Guideline 4: Planning

(1) Planning is critical to proper detection, response, casualty decontamination, and mitigation of a terrorist incident The CBRNE emergency response plan should be planned, staffed, exercised, and signed by the installation commander. Elements within the installation CBRNE emergency response plan to include CBRNE exercises should be integrated into all installation AT exercises.

(2) To plan adequately for CBRNE emergency response, the commander should:

(a) Incorporate observations and lessons learned from vulnerability assessments.

(b) Include in CBRNE emergency response planning critical infrastructure nodes on the installation and possible support, as appropriate, to critical infrastructure nodes off the installation that may affect an installation's ability to conduct its mission.

(c) Include a communication guideline for standard operating procedures with designated sequences of call signs for coordination with mutual aid partners whenever possible.

(3) Commanders at all levels should review CBRNE emergency response program and plans at least annually to facilitate program enhancement and to ensure compliance with the standards contained in this Instruction.

e. Guideline 5: Training and Exercises

(1) Fire/Emergency Medical Services (EMS)/HAZMAT training should comply with applicable requirements of the Standards for Professional Competence of Responders to Hazardous Materials Incidents and Standards for Competencies for EMS Personnel Responding to Hazardous Materials Incidents.

(a) The appropriate governing Federal, State, or host-nation regulations governing pre-hospital care providers (emergency medical services operations), both Basic Life Support and Advanced Life Support emergency medical services.

(b) Hospital care providers and medical practitioners, should comply with the Joint Commission on Accreditation of Health Care Organizations standards and the Commission on Accreditation of Air Medical Transport.

(2) Commanders shall ensure installation CBRNE emergency response exercises and training are consistent as appropriate with the established performance objectives contained within this Order.

(3) Commanders shall consider appropriate venues where emergency responder training is conducted to enhance and ensure sustainment of emergency responder skills.

(4) A CBRNE emergency response training program shall be developed and conducted on each installation by the CBRNE Protection Officer or the commander's designated person. This training should include:

(a) Appropriate standards and tactics, techniques, and procedures.

(b) An executable installation CBRNE emergency response plan designed to maintain and improve emergency responder proficiency.

(5) Commanders shall conduct annual CBRNE exercises, in conjunction with annual AT exercise, using realistic CBRNE scenarios appropriate to the installation's mission and vulnerabilities to validate the concept of operations articulated in their CBRNE emergency response plan. Scenarios should consider terrorism, technological accidents, and natural disasters that may result in CBRNE releases and incidents.

(6) Exercises should include participants from all emergency response functions on the installation and whenever possible, appropriate Local, State, Federal, and host-nation participants.

(7) When possible, commanders are encouraged to align their installation exercise and training schedules with that of the Department of Justice, the Office of Domestic Preparedness exercise and training programs for State and Local preparedness programs to include Civil Support teams (CSTs).

(8) When appropriate, OCONUS installations should align their installation exercise and training schedule with the Combatant Commanders, host-nation, and the Department of State-related CBRNE exercises.

f. Guideline 6: Emergency Response Equipment

(1) Commanders should prepare a list of needed equipment that supports capabilities for emergency response on the installation to a CBRNE incident.

(2) Equipment worn by emergency responders should comply as appropriate with Occupational Safety and Health Administration (OSHA) regulations, and National Institute for Occupational Safety and Health (NIOSH) guidelines pertaining to hazardous material response, as appropriate.

(3) Equipment requirements for each installation should be based on factors such as: priority, risk and/or vulnerabilities, and objective-level of response capability.

(4) Equipment should include both military and commercial-off-the-shelf equipment and must fall within the following categories:

(a) Protective Equipment, to include chemical protective clothing, both encapsulating and overall style suits, self-contained breathing apparatus, both closed-circuit and open-circuit, full-face air purifying respirators, and powered air purifying respirators; chemical protective gloves and chemical protective boots, cooling vests, protective headgear, and communication devices. Collective protection shelters are also included in this category.

(b) Sampling, Detection, and Identification Equipment.

(c) Casualty Decontamination and Containment Equipment.

(d) Medical Materiel, to include prophylaxis, therapeutic, and palliative pharmaceuticals, and equipment.

(e) Blast Mitigation/Containment Equipment.

(f) Communication Equipment.

(5) Commanders shall ensure, when possible, that installation emergency response equipment is interoperable with equipment used by mutual aid partners in the outside communities.

g. Guideline 7: Sustainment

(1) A large-scale CBRNE incident can quickly exhaust installation emergency responders and require the capabilities of local, State, or Federal emergency responders. In addition to training and working with local emergency responders, commanders should establish liaison with appropriate State and Federal emergency response officials to better understand whom to contact and how the integration of State and Federal assets would occur should the level of emergency response on an installation require these assets.

(2) Each installation should plan for the sustainment of its CBRNE emergency responder preparedness program.

(3) CBRNE emergency response plans should be updated, based on feedback from exercises, organizational changes, threat changes, and major world events.

(4) CBRNE emergency response training sustainment should include mechanisms to train new installation emergency responders.

(5) Commanders should incorporate CBRNE emergency response training into the curriculum of the schools and other forms of professional military education.

(6) CBRNE emergency response equipment should include requirements for sustainment, to include replenishment of consumables, spare parts, and maintenance.

(7) Coordinate with the Marine Emergency Preparedness Liaison Officer (MEPLO) to establish contact with the appropriate State and Federal emergency response officials within the installations respective FEMA region and coordinate CBRNE emergency response plans for response to a CBRNE incident on the installation.

h. Guideline 8: Assessments

(1) Identified shortfalls should be documented and resolved in subsequent steps in the preparedness program. Some critical information may need to be classified.

(2) CBRNE emergency response program elements include:

(a) Threat assessments.

(b) Vulnerability assessments.

(c) Compliance assessments.

(d) Planning and exercises.

(e) Program reviews.

(f) Training.

(3) The process or sequence of CBRNE emergency response program elements shall be iterative and serve continuously to refine the installation CBRNE emergency response plan.

(4) CBRNE emergency response programs shall be subject to continual assessments to avoid complacency. Evolving terrorism threats and changing local emergency responder conditions make periodic assessments essential.

(5) Assessment of potential threat of terrorist use of CBRNE weapons. Commanders at all levels shall take appropriate measures to protect personnel, families, facilities, and materiel, and reduce the vulnerability to terrorist use of CBRNE weapons.

(6) Commanders shall develop CBRNE threat assessments for potential terrorist use of CBRNE against personnel and assets for which they have responsibility. Reports through the chain of command should be processed immediately when significant information is obtained identifying organizations with CBRNE capabilities. A threat assessment should:

(a) Focus on the most probable terrorist threat for the facility and appropriate countermeasures. In cases where no identified threat exists, modeling and templates should be used to assess an installation's capability to implement emergency response measures under increasing Force Protection Conditions in response to an increase in the terrorist threat level or terrorist threat warning.

(b) Prepare to identify at least annually, the full range of known or estimated terrorist capabilities and possibility of non-hostile incidents for use when conducting vulnerability assessments and planning countermeasures. Threat analysis is required to adequately support risk management decisions. Terrorism threat and/or potential incident assessments should be the basis and justification for recommendations on CBRNE emergency response program enhancements, program planning, and budget requests.

(c) Be the tool that commanders use to arrive at a judgment of risk and consequences of terrorist attack or non-hostile incident. Commanders should integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources to prepare their assessments. Threat assessment for the purposes of emergency response planning is key to the overall AT force protection program.

(d) Include, as a minimum, liaison with local, State, and Federal law enforcement. In overseas locations, this

would include the country team and host-nation security, where applicable.

(7) Assessment of CBRNE Vulnerability. Commanders should conduct a local vulnerability assessment for facilities, installations, and critical nodes within their area of responsibility. The local vulnerability assessment should address the broad range of threats to the installation and its personnel and should be conducted at least annually. The Military Services and geographic Commander-in-Chiefs should ensure that the DOD component commanders conduct vulnerability assessments frequently enough to ensure that the level of response capability of installation emergency responders is sufficient to enable the installation to respond as needed to a CBRNE incident. CBRNE vulnerability assessments will normally occur at the installation commander level. Vulnerability assessments of installations should:

(a) Focus on the assessed unit's overarching preparedness program.

(b) Consider the range of identified and projected response capabilities needed for a terrorism threat against the installation, its personnel, facilities, and other critical assets.

(c) Identify response to vulnerabilities and solutions for enhanced protection of DOD personnel and resources.

(d) Provide a vulnerability-based analysis of an activity's CBRNE emergency response program. The assessment identifies for the commander, vulnerabilities that may be exploited by terrorists and suggests options that may eliminate or mitigate exploitation of those vulnerabilities.

(e) Be classified in accordance with the appropriate Security Classification Guides.

(f) Assess, as a minimum, the following functional areas:

1. The installation's CBRNE emergency response program and ability to accomplish appropriate guidelines contained in this Instruction and/or applicable prescriptive standards established by the appropriate Combatant Commanders and Services.

2. The ability of the installation to respond to the most likely CBRNE threat.

(6) Assess current personnel, resources, and equipment to respond to a CBRNE incident at each installation. This assessment should:

(a) Be conducted on organizations to include Fire and/or HAZMAT and rescue, Law Enforcement and/or Security personnel, emergency medical management, and EOD and/or civilian bomb technicians at a minimum.

(b) Include an inventory of assets on the installation as well as what is available through mutual aid assistance with outside communities.

(7) Risk Assessment. Commanders should conduct risk assessments to integrate threat and vulnerability assessment information to make conscious and informed decisions to commit resources or enact policies and procedures that either mitigate the threat or improve emergency response capabilities. Risk assessments should analyze and integrate the terrorist threat, the criticality of the assets, the vulnerability of the facility, and the strength of the installation CBRNE emergency response programs.

(a) Assessment of CBRNE emergency response programs. This assessment should determine the assessed installation's ability to protect personnel and critical infrastructure to include the full range of CBRNE emergency response from pre-incident to mitigation. Techniques include procedural measures such as, security force training, security surveys, medical surveillance for unnatural disease outbreaks and armed response to warning or detection, biological, chemical, and radiological agent detectors and filters, and other security systems. The assessment should also consider commercial-off-the-shelf technology enhancements and potential solutions for those circumstances where existing technology or procedural modifications do not provide satisfactory solutions. The assessment should examine:

1. The assessed installation's ability to determine its vulnerabilities against commonly used terrorist weapons and explosive devices. The assessment should further examine the ability to provide installation infrastructure protection against terrorist events. The ability to respond to

a terrorist event, with emphasis on a mass casualty situation, should also be examined.

2. Written plans and/or programs designed to support areas of pre-incident planning, emergency response, medical needs, equipment, law enforcement, training, intelligence support, security, and post-incident response (the ability of the activity to respond to a terrorist incident, especially a mass casualty event, to include contamination control and disease outbreak caused by terrorist use of chemical and biological weapons).

3. The availability of resources to support plans as written and the frequency and extent to which plans have been exercised. The assessment should determine the status of formal and informal agreements with supporting organizations using an MOU or MOA, Inter-Service Support Agreements, Host-Tenant Support Agreements, or other models.

4. Team Composition and Level of Expertise. As a minimum, the level of expertise and team composition must support the assessment of emergency responders for the functional areas described above. Team membership should have expertise in the following areas:

a. Emergency response.

b. Civil Support.

c. Electrical.

d. HAZMAT.

e. Special Operations.

f. Operational Readiness.

g. Law enforcement and medical operations.

h. Intelligence or counterintelligence.

i. Facility management.

j. Public affairs.

5. Specific size and certification of expertise, as directed by the Combatant Commanders and/or Service creating the team. However, team members must be functionally orientated and have experience in the assessment area to be considered for team membership.

(8) Based on site-specific factors such as Terrorism Threat Level, terrorist characteristics, geography, and security environment, assessment teams may be augmented by personnel with expertise in CBRNE weapons effects, CM, and other specialties.

i. Guideline 9: Interoperability

(1) Commanders should pursue consistency with preparedness efforts in their civilian mutual aid community or host-nation response assets to provide the necessary interoperability for successful emergency response to a CBRNE incident.

(2) Commanders should improve interoperability on installations with local communities (to include other area installations) by participating in local community exercise and training and, where appropriate, have local communities participate in installation exercise and training.

5. Levels of Emergency Response Guidelines. The levels of response capability guidelines should be incorporated in implementing documents where appropriate. The levels of emergency response guidelines are provided in Figure 1-5 on the following page.

Levels of Emergency Response

Priority Level	Objective Response Capability	Associated Equipment	Supporting Training Courses
High Priority (Technician/ Specialist Capability)	Operator's competency plus: • Ability to operate unhindered by equipment shortfalls in any contaminated environment (operators should possess needed equipment to perform tasks • Conduct safe sampling procedures in contaminated environment	• High-Level Equipment Advanced detection • Computer database references • Computer programming for detection equipment • Responder protected detection equipment	• Technician/Specialist level Hazmat (offensive/hot zone) • Specialist level Physician, Nurse, and Public Health • Emergency Assessment and Detection training
Medium Priority Operations Capability	Basic competency plus: • Operate with Hazmat teams(defensive only) • Initial detection and monitoring (defensive, not in hot or warm zone) • Establish mass casualty response/treatment systems • Establish transport for mass casualties (gross decontamination only) • Implement evacuation plans • Advanced PPE Measures (only if trained) • Conduct operations in a contaminated environment	• Moderate increase level equipment • Level A, B, & C PPE • Self Contained Breathing Apparatus •Decontamination • Detection	• Operations Level for Fire and selected Security , EMS, Public Works, physician, nurse, and public health personnel • Technicians for Hazmat or personnel who plan to work in the hot zone • CBRNE Installation Emergency Response Trainers Training & Installation Planners Training
Low Priority Awareness Capability)	• Self protective measures • Protect general population from further contamination	•IPE to include equipment, detection, and decon capabilities as appropriate 25	• Responder Awareness Course • Awareness Level all disciplines (except firefighters - minimum is operations level • Command and Staff Workshop

Figure 1-5.--Levels of Emergency Response Guidelines

Chapter 2

PROGRAM PLANNING AND CONSIDERATIONS

1. Program Planning. The Deputy Commandant (DC), PP&O has overall responsibility for coordination of the installation CBRNE protection program and for the development of policy and guidance with respect to installation CBRNE protection within the Marine Corps. The need for coordination and integration of effort between policy development, maintenance and sustainment of our installations, specific requirement generation & validation, operational testing, and systems acquisition, is more critical now than ever before. An overview of coordination and integration of the installation CBRNE protection program is depicted in Figure 2-1 below.

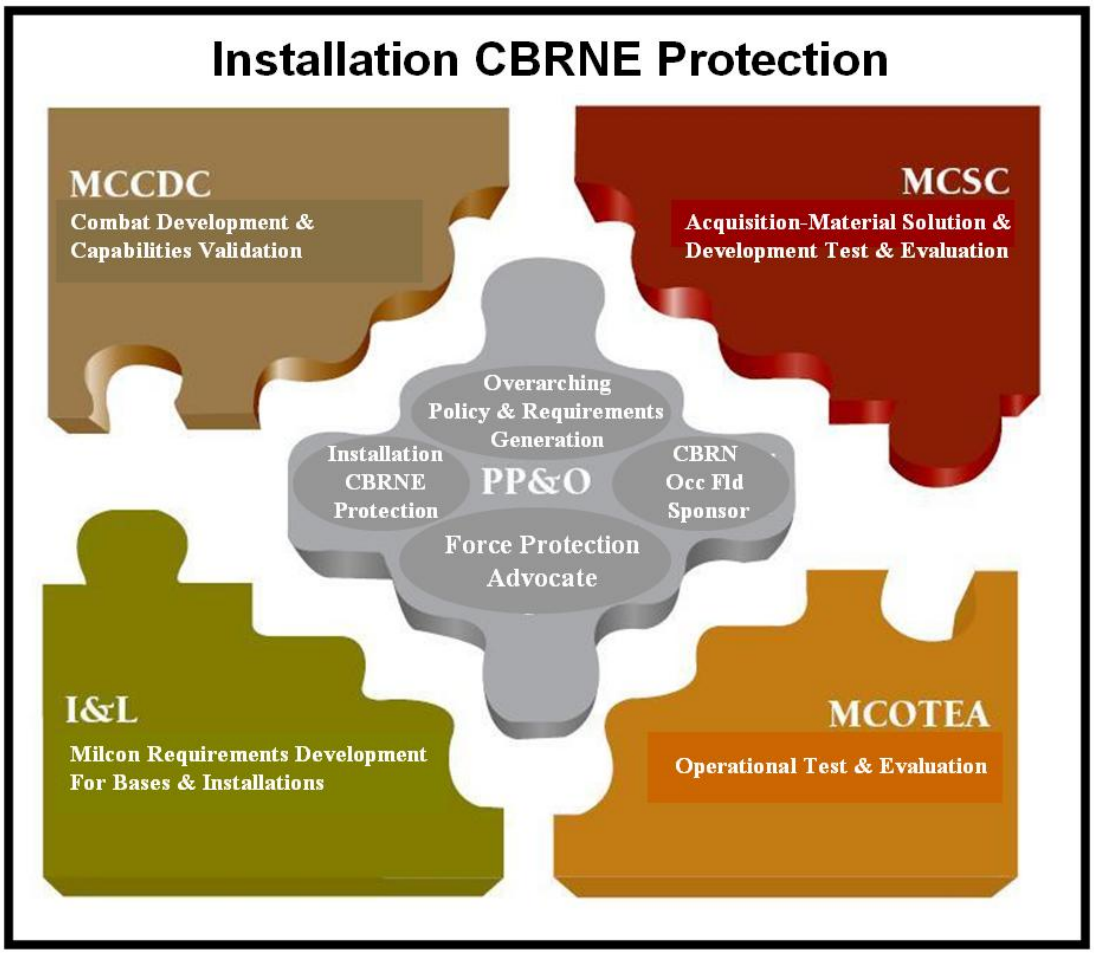


Figure 2-1.--Installation CBRNE Protection Overview

2. Installation CBRNE Protection Planning Considerations

a. CBRNE Protection

(1) CBRN warfare involves the use of Chemical Warfare Agents (CWAs), Biological Warfare Agents (BWAs), Toxic Industrial Material (TIMs), or radiological and nuclear weapons by a recognized political state during declared or open hostilities against the United States or its allies. Unlike the use of explosives and incendiaries in combat, the warfare use of chemical or biological weapons is considered a violation of the Law of Armed Conflict. Doctrine, policy, and Tactics, Techniques, and Procedures (TTPs) for CBRN warfare defense are already established and approved by all four services and current doctrine has been coordinated with the North Atlantic Treaty Organization (NATO) and other allies.

(2) The possibility exists that hostile nations, foreign or domestic terrorists, or transnational organizations will use CBRNE weapons and/or TIMs against Marine Corps installations, as well as the civilian population at-large and/or adjacent to Marine Corps installations. The possibility exists that a determined terrorist force may be successful in breaching the security perimeter of an installation and executing an attack.

(3) Should a CBRNE incident occur, it is presumed that such an incident involves or is initiated by a terrorist organization.

(4) Natural disasters can be planned for and somewhat mitigated but cannot be prevented.

(5) Response to a CBRNE attack at an installation will require all existing first responder assets (fire, hazardous material, security, explosive ordnance disposal, medical), and might exceed the crisis response and consequence management capabilities of an installation’s organic resources.

(6) For large-scale all hazards events, including CBRNE attacks, CONUS installations will require extensive DOD, Federal, State, and Local support. Installations located OCONUS will likely require assistance from host nation response assets.

(7) Close liaison with Federal, State, Local, private, and host nation emergency management officials will be essential during the planning process to ensure that civil authorities are responsive in protecting Marine Corps resources, personnel and

dependents living off installation. However, in a CBRNE incident that simultaneously affects military and civilian assets and populations, civilian/host nation assets may not be available to assist or respond to incidents affecting military installations. Total reliance on civilian/host-nation emergency response and support capabilities is not warranted or feasible in many cases.

(8) Individual Protective Equipment (IPE) and Personal Protective Equipment (PPE) required for response to CBRNE terrorism, accident, and incident events differ from that required for warfare response. This is due to differences in the nature of the threat, level of acceptable risk, and applicable safety standards.

(9) High-yield explosives may specifically not be a CBRN threat, but it is most certainly a part of the environment and conditions under which emergency response personnel are likely to perform consequence management. After a CBRNE event occurs, the scene will be littered with many challenges related to the safety of personnel conducting consequence management. These challenges will be presented not only by the after-effects of the weapons, but by the remains of those weapons that are not consumed by effects of heat and blast and must be considered in planning consequence management operations. Many delivery systems for CBRN threats include an explosive component, or may be closely associated with non-CBRN explosive devices. To ensure the success of consequence management activities under conditions where explosive or components may remain a hazard at the incident site high-yield explosives need to be amplified and considered. Although this Order does not focus on Explosive Ordnance Disposal (EOD) specifically, ignoring high-yield explosives would be ignoring an important part of the incident environment.

b. CBRN Passive Defense

(1) Passive defense operations focus on protecting assets, sustaining mission operations, and minimizing casualties during and after an attack or incident. The highest priorities for installation passive defense are force survivability and successful mission accomplishment. Passive defense vulnerability planning is supported by higher command providing available information on enemy capabilities and technical reach-back capability.

(2) The Joint Requirements Office for CBRN Defense (JRO-CBRND), the Joint Program Executive Officer for CBRN Defense

(JPEO-CBRND), and the Joint Test & Evaluation Executive for CBRN Defense (JTE-CBRND) are involved in the development of existing military response doctrine, policy, and tactics, techniques, and procedures for CBRN warfare. The CBRN Defense Passive Defense construct is depicted in Figure 2-2.

c. CBRN Active Defense. Active defense is primarily accomplished through vulnerability reduction measures. Vulnerability reduction measures are attempts to deter and deny the use of CBRN weapons by ensuring that US forces succeed in a CBRN environment and are addressed outside of the installation CBRNE protection program.

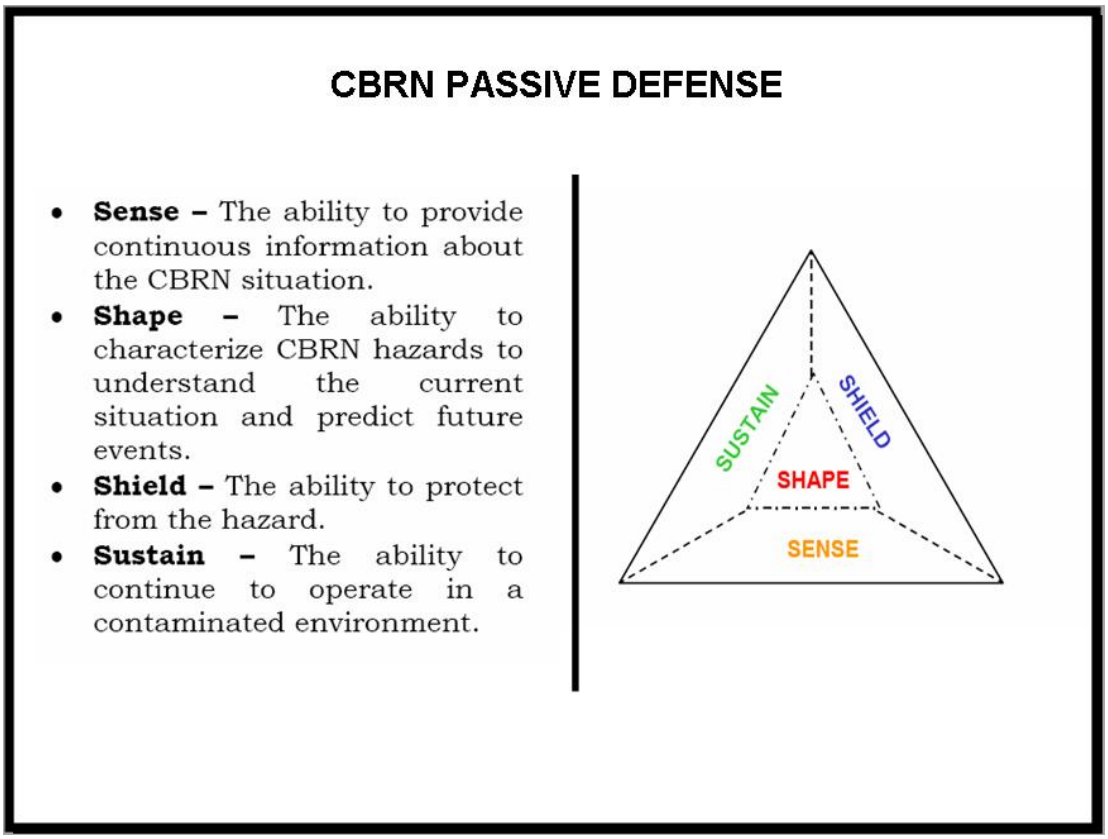


Figure 2-2.--CBRN Passive Defense Overview

Chapter 3

INSTALLATION COMMANDER PROGRAM BASELINE DETERMINATIONS

1. Initial Determinations

a. Identify and Prioritize Missions

(1) Commanders must identify and prioritize missions as follows:

(a) Identify missions in support of Combatant Commander for the deployment and projection of forces and capabilities (Priority 1 Mission).

(b) Protect all personnel on an installation (Priority 1 Mission).

(c) Identify missions in support of the Commandant of the Marine Corps' (CMC) title 10 responsibilities to train, organize, and equip the force (Priority 2 Mission).

(d) Identify missions supporting essential installation functions and day-to-day operations (Priority 3 mission).

(2) The number and type of missions identified from the above guidance will be a significant factor in determining the installation's required organic baseline capability to prepare for and respond to a CBRNE incident or other hazardous event.

b. Determine Installation Class

(1) A sound installation CBRNE protection program involves the implementation, integration, and coordination of multiple tasks and requirements. The nature and scope of the necessary tasks and requirements will depend primarily upon the size and unique characteristics associated with each installation as well as each location's contribution to the execution of critical military functions in support of one or more operations plans. Installations facilities are classified as follows:

(a) Class I – Large/Critical Installations. These are installations with a population of greater than 15,000 personnel, designated by a Service or Combatant Command because

of criticality of mission, or designated as critical through the DOD Critical Infrastructure Protection (CIP) program.

(b) Class II – Emergency Response Installations. These are installations with an emergency response capability and populations below 15,000 personnel, but more than 2,000 personnel. Class II does not contain installations, facilities or assets designated as critical through the DOD CIP program.

(c) Class III – Non-Emergency Response Installations. These are installations with populations below 15,000 personnel but more than 2,000 personnel that do not possess an emergency response capability (the installation requires support from external federal, state, or local emergency responders). Class III does not contain installations, facilities or assets designated as critical through the DOD CIP program.

(d) Class IV – Smaller Installations or Facilities. These are installations without an emergency response capability and populations of less than 2,000 personnel. Class IV does not contain installations, facilities or assets designated as critical through the DOD CIP program.

(2) The class of installation identified from the above guidance will be a significant factor in determining the priority assigned to installations for receiving CBRNE preparedness and defense equipment and training. The level of equipment and training, and thus response capability, is also determined, in part, based on the class of installation.

(3) Class I installations will be provided the highest level capability packages, and Class IV installations the minimal level capability packages.

c. Identify Critical/Essential Personnel. Commanders shall provide appropriate levels of CBRNE protection for personnel at installations and facilities, based on appropriate procedures, equipment, and training. This includes military personnel, DOD civilians, other persons who work on the installations and facilities, and family members assigned overseas or who work or live on our installations and facilities worldwide.

(1) The objective for personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host nation personnel or third country

nationals) will be to provide the appropriate level of protection to support mission continuity.

(2) For all other persons, the objective will be to provide protection or procedures necessary to safely survive an incident.

(3) Personnel categories shall be used to identify the targeted audience of specific installations CBRNE protection requirements. Commanders will focus their CBRNE resources to protect Category I-IV personnel, and providing preparedness, response, mitigation and recovery capabilities to Category V personnel. The following are definitions for the five categories of installation personnel:

(a) Category I. Emergency-Essential U.S. Military Personnel, DOD Civilians, and DOD Contractor Personnel who perform essential services, including:

1. Emergency-Essential U.S. Military Service members.

2. Emergency-Essential DOD Civilian employees per reference (s).

3. USMC contractors or employees of USMC contactors performing emergency essential USMC contractor services.

(b) Category II. Other U.S. personnel, including:

1. U.S. military family members living on and off a military installation.

2. Non-emergency essential U.S. military personnel and USMC civilian employees.

3. USMC contract employees other than those performing essential USMC contractor services.

4. Employees of other U.S. Government agencies.

5. Other U.S. Government contract employees.

(c) Category III. Other personnel supporting US Military Operations, including:

1. Personnel (non-US citizens) who are USMC employees or contractors, who are not included in Categories I and II.

2. Foreign military personnel employed by the host-nation government or by contractors of the host-nation government.

(d) Category IV. Allied/Coalition Nation Personnel, including host-nation personnel and third country nationals that the U.S. may assist pursuant to an international agreement or as directed by the Secretary of Defense, such as allied/coalition military forces, government officials, and emergency response personnel.

(e) Category V. First and Emergency Responders who are U.S. Military Personnel, DOD Civilians, and/or Contractor Personnel, including:

1. Fire and emergency services personnel, HAZMAT teams, EMS personnel, EOD teams, MTF and health care providers, Emergency Response Teams, Emergency Operations Center staff, mass care personnel, 911 call-in and dispatch staff, security forces and PMO.

2. Category V personnel may also include public works, public affairs, supply/logistic personnel, Industrial Hygiene, Occupational Safety and Health, and any other personnel designated to perform response or recovery tasks in support of the CBRNE Preparedness and Response program.

(4) CBRNE preparedness and response planning shall support the ability of Category I personnel to continue mission essential functions for at least 12 hours, at either their primary or alternate sites.

(5) CBRNE preparedness and response planning will protect Category I through- IV personnel by using a combination of personal protective equipment, shelter, shelter-in-place, safe-haven, and evacuation procedures, coupled with the employment of organized, trained, equipped, exercised and adequately sustained Category V personnel.

d. Ensure AT Plans incorporate CBRNE requirements

(1) The AT plan shall describe site-specific AT measures. AT programs shall include tenets of counter-surveillance and counterintelligence, and shall identify an appropriate organization as the focal point for the integration of local and/or host nation intelligence, counterintelligence, and criminal intelligence information into AT operations. The AT plan shall address the following key elements as they relate to installation CBRNE protection:

(a) Terrorism Threat Assessment.

(b) Vulnerability Assessment

(c) Risk Assessment.

(d) AT and Physical Security measures.

(e) Terrorist Incident Response measures.

(f) Terrorist Crisis Management measures.

(g) Terrorist Consequence Management measures.

(2) The Joint Staff J34 AT planning template may be used as a guide in preparing the AT plan.

2. Threat Assessment

a. Threat Information Collection and Analysis

(1) Commanders will task the appropriate organizations and personnel under their command to gather, analyze, and disseminate CBRNE threat information in accordance with applicable laws and DOD regulations, as well as collect information on local and regional fixed sites and transport modes that could be exploited by a terrorist.

(2) The Naval Criminal Investigative Service (NCIS) has responsibility for criminal and security investigative or counterintelligence matters with Federal law enforcement agencies. NCIS is the primary agency for liaison with state and local and foreign law enforcement, security and intelligence agencies, including those of military departments. The installation obtains local terrorist threat information from the Naval Criminal Investigation Service Resident Agent (NCISRA). Other agencies, which support and have occasion to exchange information/ intelligence include the Department of Homeland

Security, FBI (Joint Terrorism Task Force (JTTF)), State and Local police departments.

(3) CBRNE threat information should be integrated to meet the collective needs of CBRNE, AT, CIP, IA, and emergency response.

(a) Commanders should continuously ensure that forces are trained to maximize the use of CBRNE information derived from liaisons to law enforcement, emergency response, civil public safety, environment, public health, medical surveillance, intelligence and counterintelligence processes and procedures.

(b) Personnel will report information on individuals, events, or situations that could pose a threat to the security of USMC installations, facilities, personnel, families, and resources.

b. Threat Information Flow

(1) Commanders will disseminate all information (subject to release limitations) pertaining to suspected CBRNE threats or incidents involving USMC installations or facilities up and down the chain of command and laterally to adjacent and tenant units. CBRNE threat information flow should be the same as, and integrated with, other related threat information flow.

(2) Patterns of surveillance, targeting and planning are best recognized through sharing of information. These efforts will include the chain of command, adjacent units and installations, tenant units, in-transit units, and the interagency process at the appropriate level.

(3) When local information indicates gaps, commanders should forward timely requests for information via appropriate intelligence collection and production channels.

c. Installation Threat Analysis

(1) Commanders will prepare installation threat analyses at least annually or when the threat dictates for designated installations and facilities. These analyses will be a factor in justifying CBRNE enhancements, risk management, program/budget requests, and applying CBRNE measures. CBRNE analysis should be done at the same time as, and integrated with, other related threat analyses (e.g., AT, CIP).

(2) The first step in developing effective CBRNE preparedness and response capability is to identify potential hazards and CBRNE threats to the installation. Commanders who understand these hazards and CBRNE threats can better assess their ability to deter, detect, defend, and respond to a CBRNE or terrorist-exploited industrial incident.

(3) HQMC will designate which installations and facilities will prepare these Installation Threat Analyses.

(4) Installation Threat Analyses should include a liaison with local authorities.

(5) Commanders shall prepare CBRNE installation protection risk assessments at least annually for installations designated by HQMC. Commanders shall conduct CBRNE Installation protection risk assessments concurrent with other related risk assessments to include incident management actions to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. These assessments will be a factor in justifying CBRNE protection enhancements, risk management, program/budget requests, and applying CBRNE protection actions. Risk assessments will analyze the following elements:

(a) Installation threats.

(b) Criticality of installation missions.

1. Vulnerability to installation threats.

2. The ability to conduct activities to deter CBRNE incidents, employ countermeasures, mitigate the effects of a CBRNE incident, and recover from a CBRNE incident.

3. Integrated Vulnerability Assessment

a. Commanders must conduct an integrated vulnerability assessment for facilities, installations and critical assets, infrastructures and nodes within their area of responsibility on an annual basis, or more frequently as required. These assessments will include CBRNE threats posed by nearby commercial activities (e.g., chemical plants) and transportation modes (e.g., truck and rail). Subject matter experts from the related vulnerability assessments, such as CIP, incident and consequence management, and physical security should supplement

AT subject matter experts when completing Installation CBRNE Protection Vulnerability Assessments.

b. Installation vulnerability assessments will focus on evaluations of CBRNE capabilities, be subject to continual assessment, and benefit from other installation experiences. Evolving threats, technological changes, refining operational concepts, and changing local conditions make continual vulnerability assessments essential. Installation commanders will publish installation vulnerability assessments for internal use at least annually. CBRNE vulnerability assessments should be done at the same time as, and integrated with, other related vulnerability assessments.

c. Installation Vulnerability Assessment Functional Areas. Assessments will examine an installation's ability to determine its vulnerabilities against potential natural hazards, terrorist CBRNE agents, weapons, and explosive devices; industrial materials that could be exploited by terrorists; structural or infrastructure protection against CBRNE incidents and natural hazards; and installation response to natural hazards and CBRNE incidents. Installation Vulnerability Assessments will assess at least these functional areas:

(1) CBRNE Preparedness and Response Capabilities. This part of the assessment examines an installation's organic abilities and capabilities to prepare for and appropriately respond to a CBRNE incident.

(2) Installation Threat Assessment. This aspect of the assessment will focus on the ability to actively collect threat information, process that information, and develop an installation threat statement. This assessment will include fixed and mobile industrial sites/sources that could be exploited by terrorists. Further, the assessment will examine the ability to disseminate information to protect installations, facilities and family members.

(3) Installation Integrated Vulnerability Assessments.

(a) Should be completed by multiple subject matter experts, including CBRNE subject matter experts.).

(b) Should be coordinated and completed in conjunction with the HQMC and DOD CIP program standards, and the Antiterrorism (AT) Vulnerability Assessment standards.

(c) Will examine the availability of resources to support CBRNE plans as written and the frequency and extent to which plans are exercised.

(d) Will examine how plans complement one another and support the assessed installation's ability to identify changes in the CBRNE threat, implement appropriate CBRNE measures, and provide an appropriate response should a CBRNE event occur.

(e) Will examine the level and adequacy of support available from the local community.

(f) Will include food and water vulnerability to CBRNE contamination or incident.

(g) Site-Specific Characteristics. Site-specific circumstances may require assessment of additional functional areas. These additional requirements will be as directed by the commander, and should be based on site-specific characteristics such as the extent of CBRNE threats, threat characteristics, geography, and security environment.

(4) Commanders will ensure assessment teams are augmented as determined by HQMC and/or the COMMARCORBASES sponsoring the assessment. Examples of potential team members include personnel with expertise in linguistics; CBRNE weapons effects; CBRNE technology; explosive ordnance disposal; public works; firefighting; special warfare; communications; information assurance or operations; medical CBRNE defense operations, Antiterrorism, physical security, and other specialties.

(5) The installation will track and identify vulnerabilities throughout the chain of command and conduct a trend analysis to determine common issues that may need to be addressed at higher levels. At a minimum, each commander will prioritize, track, and report to the next echelon identified vulnerabilities, and actions to be taken to address vulnerabilities identified in the Installation Vulnerability Assessment.

4. Risk Assessment Process

a. Perform Risk Assessment. Commanders must estimate relative risk levels associated with specific undesirable events. Relative risk accounts for both the severity of an

event and the chance of its occurrence. Equipment, specialized material, training, and awareness affect the assessment, so the analysis requires specific information from the assessed organization and staff. Relative risk can be significantly affected by the available emergency response capabilities. An example of a risk evaluation matrix for CBRNE is depicted in Figure 3-1 below.

RISK EVALUATION MATRIX

EMERGENCY SCORE PROBABILITY AND IMPACT FROM 5 (HIGH) TO 1 (LOW AND RESOURCES FROM 5 (WEAK) TO 1 (STRONG). A LOWER SCORE IS BETTER	PROBABILITY	HUMAN IMPACT	PROPERTY IMPACT	OPERATIONAL IMPACT	INTERNAL RESOURCES	EXTERNAL RESOURCES	TOTAL
CHEMICAL							
BIOLOGICAL							
RADIOLOGICAL							
NUCLEAR							
HIGH-YIELD EXPLOSIVE							

Figure 3-1.--Risk Evaluation Matrix Example

b. Set priorities for remediation of critical asset vulnerabilities

(1) In coordination with the CIP Program Manager, identify critical assets in need of protection.
An asset is anything of value to the organization, whether tangible or intangible. Definitions are:

(a) Asset. A specific entity or unit that provides a needed service, capability, product, facility, equipment, function, infrastructure component, or other resource, or is necessary to do. Assets may be physical facilities or equipment, processes (such as software systems), or distributive in nature (such as command and control networks, wide area networks or similar computer-based networks). Assets may be privately or government owned, located worldwide, or integral to or separate from infrastructure.

(b) Critical Asset. A specific entity or unit that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department to conduct successful military operations. Impairment or loss of such entities requires near-term, if not immediate, remediation.

(2) In coordination with the CIP Program manager, assess threats to critical assets. Identify the assets affected by each undesirable event to document threats. Consider three types of threats:

(a) Natural events such as earthquakes, tornadoes or floods.

(b) Man-made events with no harmful intent such as industrial or transport accidents).

(c) Man-made events with harmful intent such as military action, terrorism or sabotage.

(3) Validate perceived threats to critical assets. This step requires replacement of intuition with a reliance on data and information obtained from research and interviews. While many sources will be classified, unclassified sources may be valuable. Less highly classified and unclassified sources permit more widespread dissemination of threat awareness information.

(4) Determine site-specific vulnerabilities for particular threats.

(a) Identify potential vulnerabilities relative to specific assets and undesirable events. Analyze installation structure and activities from an adversary’s perspective to obtain a basis for understanding true, rather than hypothetical, vulnerabilities.

(b) Many assessments involve assets that already have some protection, so this step must map threats to vulnerabilities, and vulnerabilities to assets for a consistent measurement of their interrelationships. Elements of this process include:

1. Estimate the degree of vulnerability relative to each asset and threat.

2. Assess the scope of an asset's vulnerability i.e., single weakness or points of failure, or multiple weaknesses in the protection system.

3. Assess the degree of difficulty in exploiting the vulnerability.

c. Identify risk mitigation activities and countermeasures to reduce the likelihood or severity of an undesirable event

(1) After the most serious risks have been identified, develop strategies to deter, employ countermeasures, mitigate the effects, and recover from different types of hazards and CBRNE incidents.

(2) Multiple layers of protection (defense in depth) against the most critical risks should be considered.

d. Analyze and prioritize the costs and benefits of risk mitigation strategies

(1) The final step is to identify countermeasures, costs, and tradeoffs in developing a protection strategy.

(2) The degree to which a vulnerability may be controlled and remediated is important to this protection strategy, in that:

(a) Some vulnerabilities can be remediated, eliminated or reduced before the fact.

(b) Other vulnerabilities are not within an installations control (e.g. vulnerabilities to commercial/ civilian critical assets or infrastructure that are vital to mission execution), and can not be controlled or remediated before a hazardous event or incident occurs. In such cases, liaison by the installation with the commercial or civil owner of the asset in question to discuss the vulnerability of the asset and request voluntary remediation activity by owner, is often the only course of action typically available to the installation.

5. Identify, Plan and Execute Baseline Incident Response Actions

a. Commanders shall prepare integrated CBRNE incident management actions to supplement installation AT incident

response actions, allowing response and recovery actions to continue. Commanders shall:

(1) Where multiple installations rely on common infrastructure or emergency/incident response assets in a given region, intra-service and/or inter-service support agreements shall be developed to ensure the most effective use and protection of common assets.

(2) Develop and subsequently review annually mutual aid agreements and host nation agreements as required with local emergency responders, outlining cooperative defensive actions where the military can assist civilian emergency response and vice versa during response to CBRNE incidents.

(a) Mutual aid agreements shall address specific capabilities under law enforcement, firefighting, medical surveillance, medical treatment, hazardous materials response, explosive ordnance disposal, public health, and CBRNE incident management.

(b) When applicable, mutual aid agreements must address CBRNE mass casualties.

(c) An installation’s Battle Staff (or designated alternate) shall handle requests for assistance from state and local officials when mutual aid-type agreements do not exist.

(3) Coordinate annually with civilian community emergency operations centers to identify and update responsible points of contact, emergency protocols, and expectations in the event of a CBRNE incident on or near the installation.

(4) Consider designating a Joint Information Center (JIC) to handle media demands and information control in the event of a CBRNE incident on or near the installation.

(a) Ensure policies and procedures are consistent with the U.S. Government’s “No Double Standard” policy and that procedures have been coordinated in advance with higher headquarters and any federal, local, state, U.S. mission, and host government staff elements that may be involved in its execution.

(b) If the incident is declared to be a terrorist act, then responsibility for resolving the situation may pass to another agency. If so, the gaining agency assumes the lead for

public affairs activities and the military Public Affairs Office (PAO) will act in a support role.

(5) Coordinate annually with civilian emergency response counterpart information/public affairs centers to identify and update responsible points of contact, emergency protocols, and media expectations.

(6) Be knowledgeable about the National Response Plan (NRP) and the National Incident Management System (NIMS). In coordination with the MEPLO, coordinate with and support the lead federal agencies in the event of a CBRNE incident.

(7) Determine the extent of CBRNE hazards on that installation, and determine if consistent with the CBRNE protection equipment available to the installation.

(8) Implement standard operating procedures, where appropriate, to collect samples in accordance with established sampling protocols.

(9) Be capable of rapid notification of all appropriate personnel on an installation of impending or current CBRNE hazard or incident. Note: Outside CONUS, this includes sponsored dependents living off-site.

(10) Be capable of activating appropriate medical responses (e.g., prophylaxis, vaccines, diagnosis, treatment, etc.) to a CBRNE hazard or terrorist incident.

Chapter 4

CONCEPT OF OPERATIONS (CONOPS)

1. Overview

a. In conjunction with the DOD and the DON, the Marine Corps will establish and implement a concept of operations that will focus on installation CBRNE protection capabilities that can be developed and implemented at installations and integrated into existing Anti-Terrorism (AT) plans, vulnerability assessments, and natural disaster plans. An example of an installation CBRNE Protection CONOPS is depicted in Figure 4-1.

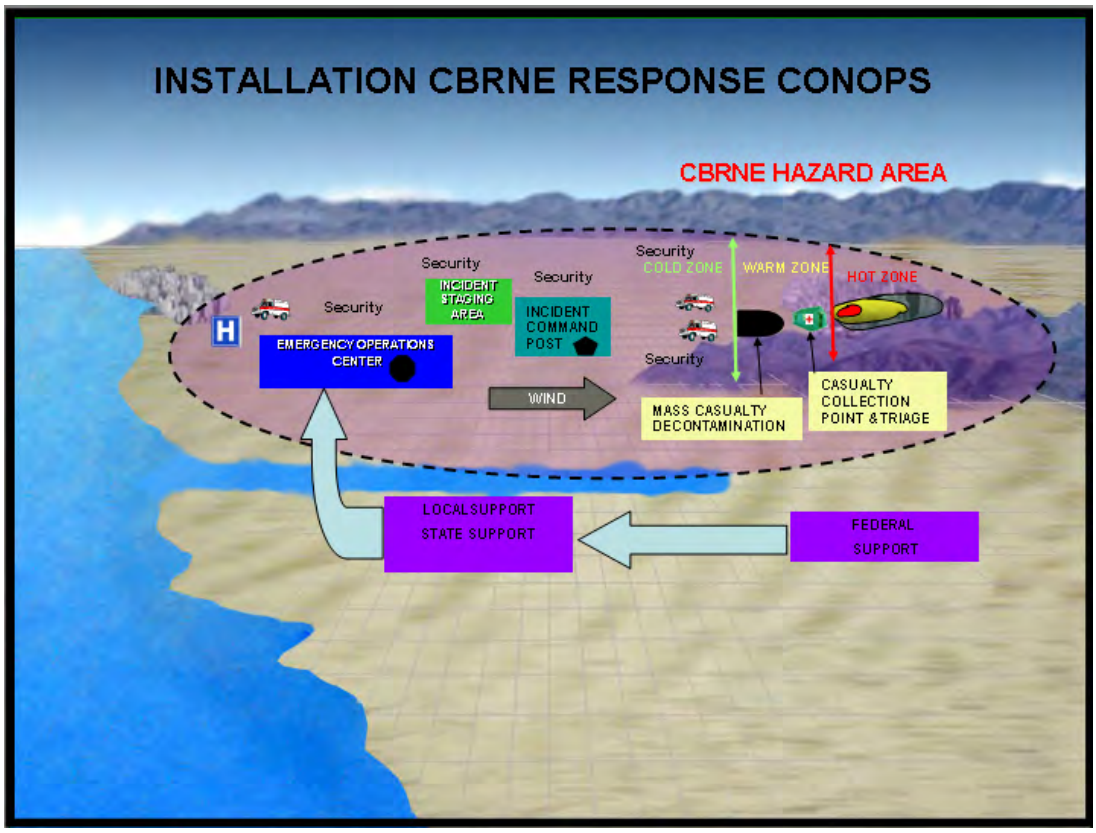


Figure 4-1.--Installation CBRNE Protection CONOPS

b. The lines of communication to be utilized for the installation CBRNE protection program are depicted in figure 4-2 on the following page:

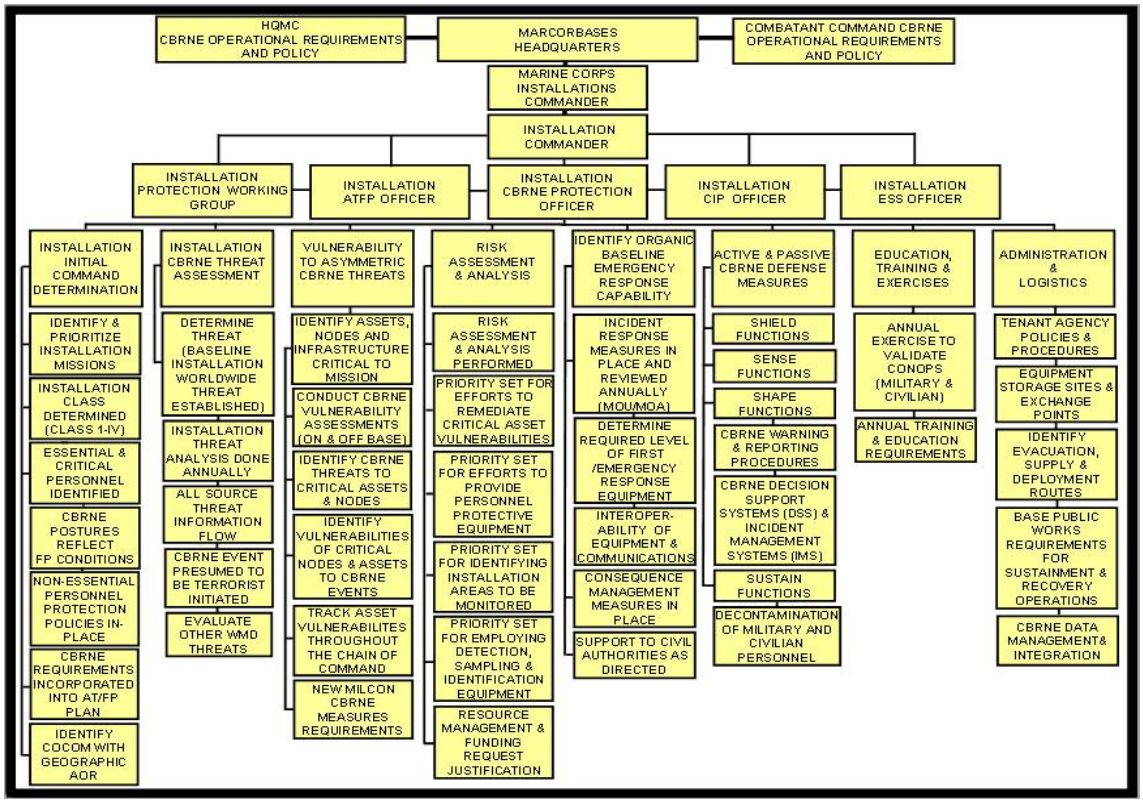


Figure 4-2.--Lines of Communication for Installation CBRNE Protection Program

2. Installation CBRNE Protection Phases

a. Installation CBRNE protection shall be organized into five separate phases which include Planning (Mitigation/ Prevention), Preparation, Response, Recovery, and Consequence Management as depicted in Figure 4-3 below.

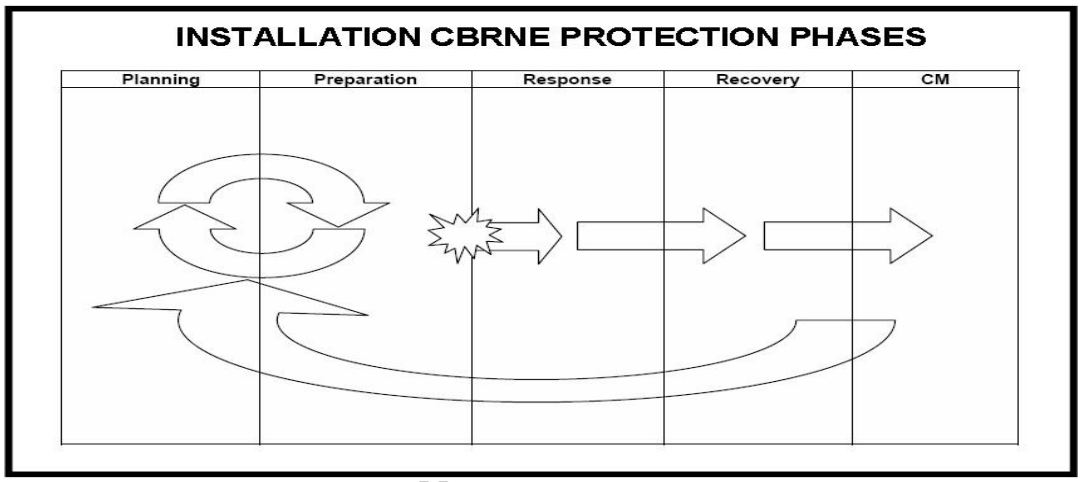


Figure 4-3.--Installation CBRNE Protection Phases

b. These five phases shall be integrated into existing installation AT plans to detect, assess (decide & task), warn, defend (active & passive), and recover from natural or man-made disasters, terrorist attacks, or criminal acts

(1) Pre-incident operations include planning and preparation phases that are executed day-to-day aboard installations, 24 hours a day, 7 days a week. A CBRNE Preparedness and Response Metric is provided in Appendix A.

(2) Incident response operations include response and recovery phases when an incident occurs on an installation and operations are then focused on a measured response, while the planning and preparation for the possibility of another incident continues.

(3) Post-incident operations include Consequence Management operations focused on reconstituting the installation response and recovery capabilities after an incident.

3. Pre-Incident Operations

a. Planning Phase. Planning for installation CBRNE protection involves the development of an installation CBRNE emergency response plan. The CBRNE emergency response plan should be part of the installation's overall emergency response plan. As new vulnerability reduction measures are completed, the plan may be modified to include improved installation CBRN defense readiness and preparedness. The CBRNE response plan is supported by the medical portion of the installation emergency response plan. Plans must be nested horizontally in case of supporting civil agreements and vertically in case of higher HQ considerations. Plans must consider and be consistent with the National Response Plan (NRP) and National Incident Management System (NIMS). The planning phase is the largest phase of installation CBRNE planning and operations, as it integrates force protection program management; risk/threat assessment; incident response and consequence management planning; equipment acquisition and construction considerations; awareness training; incident response training; and Field/Command Post exercises.

(1) The risk assessment and risk management process is the foundation upon which installation CBRNE Protection is developed. This process begins with as threat assessment, followed by an asset criticality assessment, a vulnerability assessment and culminates into an overall risk assessment that resources can be applied to. The risk assessment process, to

include threat, criticality, and vulnerability assessments, will be conducted annually.

(2) CBRNE planning is an iterative process that needs to remain flexible to an ever-changing threat environment. Initial and sustained response to a threat must be a coordinated effort between the many FP planning and response elements of the installation, based on the installation's organic capabilities. As the situation exceeds the installation's capabilities, it must activate MOAs/MOUs with the Local/State/Federal agencies within the U.S.

b. Preparation Phase. The preparatory phase incorporates a range of measures, actions, and processes to be accomplished before an incident occurs. Preparedness measures may include determining the appropriate mission-oriented protective posture (MOPP)/Personal Protective Equipment (PPE) and conducting technical reach-back, planning, training, exercises, qualification and certification, and equipment acquisition. Preparatory actions serve to ensure that pre-incident actions are standardized according to the installation's emergency response plan. Installation preparatory actions include tenant and transient units during training events. Interoperability of installation measures is also critical (e.g., an interoperable installation emergency response system that supports effective communications and synchronized response actions). Specialized installation capabilities are also exercised.

(1) Equipment acquisition and construction considerations are actions to mitigate specific vulnerabilities identified within the risk assessment and to meet minimum DOD force protection construction standards.

(2) Awareness training is an important facet of the CBRNE preparedness and response program to ensure each and every individual on the installation is aware of the potential threats and the appropriate individual protective measures.

(3) Incident Response Training ensures that all first responders, fire, law enforcement, EOD, and medical personnel have been provided appropriate initial response training and sustainment training to be prepared to respond to an incident at any time.

(4) Force Protection exercises shall be conducted annually and supplemented with tabletop exercises for a variety of specific threat situations to include a CBRNE response.

4. Incident Response Operations

a. Response Phase. The response phase addresses the short-term, direct effects of an incident. Response measures include those actions taken to save lives, protect property, and meet basic installation functional requirements. Response actions also include the execution of the installation emergency response plan.

(1) The installation moves into the response phase upon an incident occurring and operations are then focused on a measured response while pre-incident operations continue in preparations for the possibility of another incident occurring. Military Police and Fire Department personnel will generally be among the first units to respond to an incident, and will assume full control over the incident providing an incident commander/on-scene commander.

(2) The incident commander/on-scene commander will utilize the Incident Command System (ICS) for organization and execution at the incident site. The focus of incident response is to gain control, assess the situation, treat and evacuate injured/threatened personnel, contain the incident and mitigate the impact. Refer to Figure 1-4 on page 1-10 of this Order.

(3) Based upon the degree of severity of the incident, incident response may include the activation of Mutual Aid Agreements with local civilian Fire and Emergency Services, the activation of the Emergency Operations Center (EOC), the activation of the Command Center, the activation of inter-service support agreements (ISSAs), if necessary the activation of County/State/Federal emergency response plans as a regional response, and the activation of a Regional Operations Center (ROC).

(4) The severity of the incident or the type of incident may even require the activation of the Federal Response Plan with a Lead Federal Agency (LFA) being identified. The LFA will be in charge with all other agencies in support. Within the U.S., the FBI is the LFA for acts of terrorism and FEMA is the lead federal agency for consequence management during a large natural or man-made disaster. Marine Corps installations would be in a supporting role in this larger regional response.

(5) Provide OPREP-3SIR (Serious Incident Report) reports to the CMC, through the Marine Corps Operations Center (MCOC),

with information on significant CBRNE events or incidents. Refer to reference (i) and the format in Appendix C.

5. Post Incident Operations

a. There is no clear cut distinction as to where the response phase ends and recovery phase begin. Generally, as the incident response moves from an emergency response, focused on saving lives and mitigating the impact of the incident, to a planned long term response focused on recovery and reconstitution, the recovery phase begins. The plans for this phase are normally made during the response phase and when the planned assistance arrives the recovery phase begins.

b. The recovery phase includes the reconstitution of installation and tenant command capabilities; damage assessment and recovery; documentation of the incident; and request for reimbursement of funds expended. Short-term recovery returns vital life support systems to minimum operating standards. Long term recovery may go on for years until the entire disaster area is completely redeveloped, either as it was previously or in a new, less disaster prone configuration. Some examples of Post Incident actions are:

(1) Restoration of installation support services.

(2) Restoration of telecommunication services.

(3) Debris and/or HAZMAT cleanup and disposal.

(4) Resettlement of personnel evacuated from on-base housing.

(5) Counseling programs.

(6) Reconstruction/New Constrution.

c. Consequence Management (CM). The CBRNE aspects of CM include those actions taken to mitigate the effects of a CBRN attack or event and restore essential operations and services. The Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical Aspects of Consequence Management provide information that addresses this phase. Representative actions that may occur during this phase include decontamination and coordination with Federal and Host Nation agencies that may support the cleanup as part of a coordinated interagency effort.

6. Installation CBRNE Protection. CBRNE preparedness and response planning comes with a specific operational framework that will be implemented at installations as follows:

a. CBRN Passive Defense Measures. There are four functions related to CBRN Passive Defense. Refer to Figure 2-3 on page 2-4. Each pillar of the CBRN Passive Defense functional area contains specific CBRN defense measures.

(1) Sense Function. Provides and implements a continuous, real-time capability to assess the current CBRNE situation by detecting and identifying CBRN hazards in air, in water, and on land to personnel, equipment, and facilities as well as the physical state of those hazards (solid, liquid, and/or gaseous). This element includes the capability to diagnose, quantify, and sample CBRN hazards.
Taking into account installation characteristics and missions supported, commanders must:

(a) Develop, maintain, and execute CBRN protection tactics, techniques, and procedures to include “sense” operational concepts.

(b) Realize a CBRN incident occurred.

(c) Determine immediate CBRN hazards and define hazard locations.

(d) Identify the CBRN hazards involved.

(e) Plan installation sensor locations, testing procedures, and C4I to support those testing locations.

(f) Be prepared to preserve CBRN evidence, collect CBRN samples in accordance with established sampling protocols for CBRN incidents, and implement appropriate CBRNE chain of custody rules.

(2) Shape Function. Provides the capability to characterize the CBRN or other hazards to the joint force commander through manual and automatic collection and assimilation of CBRN information from a variety of sources in near real-time. This allows the commander to direct personnel to take action and provides actual and potential impacts of CBRN hazards. Taking into account installation characteristics and missions supported, commanders must:

(a) Develop, maintain, and execute CBRN protection tactics, techniques, and procedures to include “shape” operational concepts

(b) Develop and maintain CBRN protection emergency response guidelines in accordance with reference (e).

(c) Distinguish critical, essential, and other missions and operations to support Sense, Shield, and Sustain operational determinations.

(d) Assess CBRN incidents as they develop and notify local, state, federal, host nation and Service emergency response agencies as appropriate.

(e) Be prepared to transition installation CBRN incidents to federal control and then back to DOD control for long-term restoration and recovery.

(f) Identify potential temporary disposal sites for hazardous waste generated by a potential CBRN incident, as appropriate.

(3) Shield Function. Provides the capability to the joint force to maintain a high operating tempo while preventing or minimizing casualties under CBRN hazard conditions by reducing the threat, reducing operational vulnerability, and avoiding contamination. Further shielding is provided by physical protection and medical pre-treatment. Taking into account installation characteristics and missions supported, commanders must:

(a) Develop, maintain, and execute CBRN protection tactics, techniques, and procedures to include “shield” operational concepts.

(b) Protect personnel as appropriate from a CBRN incident, based on factors outlined in Chapter 2, including DOD/USMC mission criticality.

(c) Plan medical countermeasures for CBRN incidents.

(d) Be prepared to handle contaminated casualties (psychological, injured, or fatalities) both at the incident site and at military medical facilities.

(e) Suppress residual CBRN hazards while protecting evidence.

(4) Sustain Function. Despite contamination avoidance efforts, forces may become contaminated and may have to operate in a contaminated environment. Decontamination, collective protection, and medical intervention enable the quick restoration of combat power, enable the recovery of essential functions that are free from the effects of CBRN hazards, and facilitate the return to pre-incident operational capability. Taking into account installation characteristics and missions supported, commanders must:

(a) Develop, maintain, and execute CBRN protection tactics, techniques, and procedures to include “sustain” operational concepts.

(b) Continue critical missions within contaminated environments presented by CBRN incidents, if possible.

(c) Restore essential operations quickly following CBRN incidents.

b. WMD Consequence Management (CM). WMD Consequence Management (CM) is one of the eight military missions within the Combating Weapons of Mass Destruction (CBT WMD) construct and is significant function in the installation CBRNE protection program. An overview of the CBT WMD construct is provided in Figure 4-4. on the following page.

Figure 4-4.--Overview CBT WMD Military Mission Areas

(1) WMD Consequence Management consists of measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by the consequences of terrorism.

c. CBRN Active Defense. Active defense vulnerability reduction measures are attempts to deter and deny the use of CBRN the use of CBRN weapons by ensuring that US forces succeed in a CBRN environment and are addressed outside of the installation CBRNE protection program.

7. Required Level of Preparedness and Response Capability

a. Equipment and Training. The level of equipment and training, and thus response capability, must also be determined based on the class of installation. Consequently, the Marine Corps will establish and implement the following four levels of response capabilities for installations:

(1) Level 1. A basic capability package that will be implemented by all installation classes, which includes the following:

(a) No direct sensor capability is required. The installation relies on medical surveillance information for detection/identification of CBRNE hazards not readily apparent.

(b) Installation command centers receive HAZMAT software packages and a link into civil emergency management centers.

(c) Protection for civilians involves development of evacuation plans and mass decontamination using firefighting equipment.

(d) Installation emergency response teams receive increased capabilities to respond to CBRNE hazards, including level A suits, detection equipment medical, and decontamination supplies for the team (not the installation).

(e) Installations have no consequence management capability other than relying on Federal/State/Local response from outside the installation.

(2) Level 2. A supplemental capability package that will be implemented by installation Classes I-IV in addition to Level 1 capabilities:

(a) Installations shall develop and implement a mass-alert/notification system. For OCONUS, this requirement includes coverage of off-base personnel as well.

(b) No direct sensor capability outside of high-value assets, such as command centers and living areas is provided. Security personnel guarding installation gates and high-value assets will be provided the capability to detect and/or identify chemical and radiological contamination.

(c) Medical centers will be networked into a national medical surveillance system.

(d) DOD emergency/essential civilians/military receive National Institute for Occupational Safety and Health (NIOSH) approved personal protective equipment.

(e) Access to a local or regional laboratory to provide confirmatory testing of biological samples.

(3) Level 3. An intermediate capability package will be implemented by installation Classes I-III in addition to Level 2 capabilities:

(a) Personnel not executing emergency/essential missions receive shelter-in-place equipment list and instructions for residences and/or offices.

(b) An organic HAZMAT/CBRNE response team is activated.

(c) Installation medical clinics and hospitals receive the capability to decontaminate ambulatory and non-ambulatory contaminated patients.

(d) Medical laboratory capability is increased to develop surveillance and diagnostic capability.

(4) Level 4. A full capability package will be implemented by installation Classes I-II in addition to Level 3 capabilities:

(a) Installations install sensor networks connecting a number of automated point chemical and biological detectors and air samplers.

(b) All personnel, including those not executing emergency/essential missions, shall receive escape masks or will be evacuated and directed to shelter in place during a CBRNE incident.

(c) Installation medical clinics and hospitals stockpile medical countermeasures; installation response teams stockpile operational decontamination applicators and materials to continue restoration of installation functions.

b. First/Emergency Responder Training. Emergency responders must be prepared to respond to the effects of a CBRNE incident to preserve life, prevent human suffering, mitigate the incident, and protect critical assets and infrastructure.

(1) Commanders shall structure installation emergency response capabilities to include the following functional areas:

(a) C2 communications.

(b) Law enforcement/security.

(c) Fire and hazardous material, atmospheric monitoring and detection, sampling and chain of custody.

(d) Casualty extraction.

(e) Decontamination.

(f) Health and medical response, to include medical surveillance and medical management.

(g) EOD operations.

(h) Mortuary affairs.

(2) The Marine Corps, while providing all installations with a minimum of Level 2 equipment, will provide its emergency responders with training sufficient to meet Level 3 response requirements.

8. Key Concepts and Organizations

a. Crisis Management

(1) Crisis Management consists of those measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat, hazard or act of terrorism.

(2) U.S. law assigns primary authority to the Federal Government to prevent or respond to terrorism. State and local governments provide assistance as required.

(3) Crisis Management involves post-incident roles including the collection of evidence, securing the crime scene, and protecting first responders from secondary devices or follow-on attacks.

b. Incident Response Command and Control

(1) Unified Command System (UCS). The UCS will be utilized during all incidents. The system provides an integrated span of control for single or multiple terrorist

incidents involving the same senior representatives from Federal, Military, State, Local, and private agencies.

(2) National Incident Management System (NIMS). The NIMS will be utilized during all terrorism incidents. The system provides a consistent nationwide template to enable all government, private-sector, and nongovernmental organizations to work together during domestic incidents.

(3) Incident Command System (ICS). The ICS will be utilized during all incidents. The ICS provides for coordinated response and a clear chain of command for integrated, safe operations. The ICS is mandated for use at the scene of all HAZMAT and CBRNE incidents by the NRP.

(a) The ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, with the responsibility to manage resources to effectively accomplish stated objectives pertinent to an incident. Although developed specifically for the fire service, the principles of the ICS can be applied to CBRNE incidents and emergencies.

(b) The ICS is used throughout the United States and is the recognized standard for on-scene incident management. ICS is specifically designed to allow response agencies to adopt an integrated organizational structure equal to the complexity and demand of single or multiple incidents without being hindered by jurisdictional boundaries.

c. Incident Commander (IC)

(1) The IC is in charge of the incident site, and is responsible for all decisions to manage the incident, including tactical planning and execution. The IC shall have the capability and authority to:

(a) Assume command.

(b) Assess the situation.

(c) Implement the emergency action plan.

(d) Determine and implement response strategies.

(e) Determine need for outside assistance.

(f) Activate resources.

(g) Order evacuation of hazardous scene.

(h) Oversee all incident response activities.

(i) Declare that the incident is “over”

(2) Identification of the IC in the CBRNE plan. For CBRNE events, the initial IC will normally be the Senior Fire/Law Enforcement Official on scene. For covert events involving unknown disease outbreak, the senior medical officer will normally be the IC.

d. Emergency Operations Center (EOC)

(1) The EOC is the centralized operations center for emergency management at an installation. The Command Staff assembles at the EOC to analyze the situation and make decisions based on information provided by the IC and other personnel. Regardless of size or process, every installation shall designate a primary and alternate area where decision makers should assemble and conduct operations during an emergency. The EOC is an essential component of the effective use of both NIMS and the Unified Command System.

(2) Locate the primary EOC in an area of a facility not likely to be involved in an event based on results of the vulnerability analysis.

(3) Designate an alternate EOC in the event that the primary EOC location is not usable.

(4) Each facility must determine its specific requirements for an EOC based on the functions to be performed and the number of people involved. The EOC should preferably be a dedicated area equipped with communications equipment, reference materials, activity logs and other tools necessary to respond quickly and appropriately to an emergency.

9. Operational Constraints

a. Posse Comitatus Act (PCA). Although Fire and Medical services can easily be provided by the installation in support of mutual aid agreements with the local community, Law Enforcement (Military Police) and Marines personnel in general

cannot be utilized in a law enforement role off the military installation due to the PCA, title 10, and DOD policy.

b. Intelligence Oversight. There are specific limitations placed on military organizations in reference to intellgence and information gathering activies within the borders of the United States.

Note: Nothing within this section is intended to override existing event-specific command and control procedures or requirements, especially in the areas of health service support and radiological/nuclear accident/incident response.

Chapter 5

CONOPS VALIDATION: TRAINING AND EXERCISES

1. Overview

a. Training and Exercises. Commanders shall:

(1) Conduct regular field and staff training, as well as exercise integrated AT and CBRNE preparedness and response plans at least annually.

(2) CBRNE protection training and exercises will be executed in accordance with references (e) and (f), and should include Local, State, Regional, Federal, and/or Host Nation agencies.

(3) CBRNE protection training and exercises shall be integrated into AT training and exercises and CBRNE protection shortfalls shall be identified concurrently with AT shortfalls. To incorporate lessons learned, commanders shall maintain exercise documentation for at least two years.

b. Annual Exercise to Validate CONOPS. Commanders shall:

(1) Plan, prepare, and conduct integrated CBRNE preparedness and response exercises annually in conjunction with local authorities to test and validate installation preparedness and response CONOPS.

(2) Have the capability to respond to emergencies shall be evaluated in order to ascertain proficiency.

(a) The type and scope of exercises to be conducted shall be based on the vulnerability and risk assessments applicable to the region and installation.

(b) Joint exercises with local civilian agencies shall be conducted where feasible. These exercises may consist of table top seminars.

(c) Response deficiencies shall be documented and shall serve as the basis for initiating corrective actions.

(3) Design training and exercises to test, at a minimum, both military and civilian activities normally associated with the initial response to a mass casualty CBRNE incident, such as:

(a) Site characterization.

(b) Victim extraction.

(c) Treatment and decontamination.

(d) Agent identification.

(e) Site security and control.

(f) Render-safe procedures for devices/weapons.

(g) Crime scene/evidence collection, sampling and chain of custody procedures.

(h) C2 procedures.

(i) Military-Civilian coordination and communication.

(4) Design CBRNE exercises to reveal strengths and weaknesses in CBRNE emergency/first response planning and execution. Lessons learned from these exercises should:

(a) Lead to the development or modification of military/civilian response protocols and concepts of operations.

(b) Identify the need for expanded and continuous first responder training.

(c) Facilitate and coordinate the use of civilian medical surveillance programs, as well as veterinarian medical surveillance.

(d) Identify joint planning issues relating to mass decontamination and quarantine scenarios.

(e) Incorporate one or more scenarios that simultaneously attack critical infrastructure or assets, such as vital communications systems, as part of each overall CBRNE exercise. To incorporate lessons learned, commanders shall maintain per reference (l) SSIC 1510.3 for enlisted personnel, SSIC 1520.1 for Officers, and SSIC 12410.14 for Civilian personnel.

c. Annual Training and Education Requirements

(1) Response teams shall receive training commensurate with their assigned responsibilities.

(a) Initial training shall focus on providing required core competencies.

(b) Refresher training shall focus on maintaining proficiency.

(c) Emergency Responder training shall be consistent with reference (e).

(d) For CBRNE terrorism and accidents/incidents, training will be compatible with the training required by civilian emergency response agencies to assure compliance with Occupational Safety and Health Administration (OSHA) and NIOSH standards and for integrated, consistent response.

(2) General Education and Training

(a) Installation personnel and dependents shall receive training commensurate with the anticipated local threat and risk scenarios, and consistent with the type of IPE provided to them.

(b) In accordance with reference (e), the installation AT training plan shall contain integrated CBRNE protection training.

(3) MARCORBASE Commanders shall enable and facilitate additional training for CBRN Military Occupational Specialty (MOS) positions that will focus on providing knowledge of installation AT measures, procedures, and response activities.

Chapter 6

ADMINISTRATION AND LOGISTICS

1. Additional Installation Planning Guidance

a. Mass Casualty Plan. Shall be developed and maintained by the base medical clinic (BMC) or medical treatment facility (MTF). The plan should address where patients will be sent by priority, and where medical support requests will be forwarded in the event of a CBRNE incident.

b. Mass Fatality Plan. An installation-wide plan shall be co-developed by the installation senior medical official and the Logistics Department. The plan should address where and how contaminated remains will be stored. The records described in this paragraph shall be maintained per reference (l) SSIC 3000.5a.

c. Non-Combatants Evacuation Operation (NEO)(OCONUS Installations) Plan. Commanders must plan for the evacuation of nonessential military personnel, selected host-nation citizens, and third country nationals, whose lives are in danger in a host foreign nation, to an appropriate safe haven and/or the United States. The Department of State (DOS) is responsible for NEO. forward-based Navy/Marine Corps forces may be tasked to implement NEO. Combatant Commanders are responsible for planning and conducting NEOs to assist the DOS. Non-Combatant Commanders shall maintain the records described in this paragraph per reference (l) SSIC 3000.5a.

2. Construction Standards and Considerations

a. Installations shall adopt and adhere to common criteria and minimum construction such as new construction, renovation, or rehabilitation standards to mitigate CBRNE protection vulnerabilities and threats.

3. Medical/Equipment Storage Sites and Exchange Points. CBRN Medical Stockpiles. Installations shall plan for the procurement, receipt, storage, availability and dispensing of CBRNE medical stockpiles sufficient to treat CBRNE casualties within the first few hours of an incident.

a. The nature and scope of medical stockpile requirements for each installation shall be determined by:

b. Installation population.

c. Number of local providers of required medical stock.

d. Geographic location of the installation to other providers.

e. In a CBRNE event, the limiting factors will be the number of providers and the capability of installation medical facilities – not the number of casualties. Patient throughput is a constraint.

f. No immediate requirement for radiological treatment stockpile. Must provide critical medical materiel capable of responding to a chemical/biological (CB) event based on subparagraphs (a) through (c) above.

4. CBRNE Protection Considerations for Mail

a. Installations shall adopt and adhere to postal criteria and standards to mitigate CBRNE protection vulnerabilities and threats.

b. Installations shall develop preventive measures and procedures against the introduction of CBRNE laden mail from entering the installation’s mail handling systems.

c. Installation mail handling facilities shall develop formal, site-specific, procedures for reacting to suspected CBRNE package.

d. Installation Commanders shall maintain the records described in this paragraph per reference (l) SSIC 3000.5a.

5. CBRNE Recovery and Containment Operations

a. Recovery Operations Planning Considerations

(1) Response is the emergency action period in which the installation restores vital functions while protecting against further damage or injury. Recovery involves the short and long-term activities necessary to restore the installation to normal operations.

(2) Recovery begins when the incident has been stabilized and the last living victim is delivered to a medical facility to receive definitive medical treatment. It concludes

with the end of consequence management operations, which may consist of, but are not limited to or required to include depending on the unique nature of each event, public assistance, mass care, restoration of services, debris removal, re-occupancy, and remediation. The focus is on restoring mission capability and essential public and government services interrupted by the event. It is quite likely that Federal, State, Local, Private, Host Nation and other outside agencies will provide assistance during this stage.

(3) Safety is a paramount concern in any incident response. Safety during mission execution is crucial to successful operations. Recovery personnel must also be equipped with appropriate personal protective equipment PPE as required by the current installation situation and environment. PPE is heavy and cumbersome, decreases mobility and dexterity, lessens visual and audio acuity, increases physical exertion, and may increase task accomplishment time. Accordingly, commanders must plan for work-rest rotation of both first responders and recovery personnel and for recall of off-duty personnel needed to implement the plan.

(4) Environmental Considerations

(a) The IC shall coordinate with the Environmental Department and Industrial Hygiene representative during their assessment of the severity of a release to determine:

1. The nature of the release.

2. The pathways of human exposure and atmospheric conditions affecting characterization of the release.

3. Consideration of potential long- and short-term health effects associated with hazardous substances identified at the incident site.

4. Comparison of existing morbidity and mortality data on diseases suspected to be associated with the observed levels of potential human exposure.

(b) Navy/Marine Corps industrial hygiene and safety personnel shall be utilized, whenever possible, in the selection and establishment of acceptable re-occupancy standards and in the provision of assessment documentation prior to Marine Corps personnel returning to work or live in areas previously

determined to be contaminated by established detection and identification methods.

(c) There are many potential methods for handling contaminated soil, water, and sediment. Short-term recovery planning should concentrate on temporary containment of contamination (including used decontamination equipment and solutions) and isolation of contaminated items and areas. Assistance in environmental remediation technical issues can be obtained through the Navy Environmental Health Center.

(5) Mass Notification/Media Plan Psychological Considerations

(a) A largely unprotected installation population is likely to react strongly to a CBRNE attack, terrorist event, or accident/incident. Anticipate problems with crowd control, panic, and opportunistic crime. To prevent panic, resolve confusion, and allay fear, commanders must implement an effective Mass Notification and Media plan information management campaign. Early intervention and statements by command leadership and technical experts can instill confidence in the command's response to the incident.

(6) Critical Incident Stress Management

(a) Disasters have tremendous emotional and psychological impact on responders and recovery personnel as well as victims. Recovery planning must include psychological services for affected individuals. These services need to be available and provided early in the course of the disaster. This will help responders express anxieties, and provide a mechanism to identify individuals in need of further counseling.

b. Sustainment Operations Planning

(1) Personnel

(a) A CBRNE incident will be labor intensive, so commanders must ascertain the quantities and capabilities of healthcare and response/recovery personnel and resources. Ensure that personnel who provide part-time support to different agencies are not counted twice in the inventory of resources. In preparing for an event, vaccination/immunization of key healthcare and response/recovery personnel should be conducted in accordance with Navy/USMC policy and should be closely monitored by the commander through their cognizant MTF or BMC.

Ensure that critical personnel listings, such as those required for specific force protection conditions, identify and permit access to those personnel required for post-event actions.

(b) A CBRNE event, especially a biological incident may last for weeks resulting in an exhausted workforce. Plan for rest and recuperation. First responders and recovery personnel must have adequate personal protective equipment, medical and psychological support, and training.

(2) Sustainment includes maintaining food, water, power, heat and shelter, as well as efforts to maintain general public health and safety. Coordinate with local authorities to advise the community on actions to take to assure its protection, such as quarantine, closures of businesses and schools, cancellation of public gatherings, and establishment of no-entry zones or evacuation routes.

c. Decontamination

(1) The incident commander establishes decontamination priorities.

(2) First responder and casualty decontamination are integral to the response phase. Decontamination during the recovery phase is long term, more complex, and must address priorities, resources, safety, long-term health issues, environmental concerns, and effect on mission accomplishment.

(3) Decontamination of fixed sites, facilities, and terrain is resource intensive and should only be considered when operational degradation is unacceptable and mission accomplishment is at risk. Several techniques and procedures are available depending on the site and conditions. Limit decontamination to those facilities and portions of facilities that are absolutely mission-essential. Appropriately mark remaining sites and facilities, and decontaminate as necessary and as time and resources permit.

(4) Personnel participating in decontamination must receive a follow-up medical assessment.

d. Restoration and Retrograde

(1) Restoration begins upon completion of the survey for contamination and continues until all contamination has been

remediated. The scope and duration of the remediation depends on the agent or material.

(2) Retrograde movement consists of the redeployment of personnel and equipment and begins as soon as objectives are accomplished or the need for response forces diminishes.

(3) Goals for contaminated materiel retrograde are mission support, protection of forces and resources from CBRN hazards, and the control of contamination.

e. Remediation

(1) Remediation operations follow neutralization and removal of CBRN contamination. Imminent threats to personnel or the environment should be alleviated during neutralization and removal operations so remediation operations will normally take place in a non-emergency setting.

(2) Remediation is normally performed by civilian environmental consultant firms under contract to the Service and/or under the supervision of the Environmental Protection Agency (EPA), depending on the nature of the event. Funding for contract support would be provided through installation operations and maintenance (O&M) accounts, unless special appropriations are received.

7. CBRNE Data Management and Reporting Integration/Decision Support. Installations are required to document and maintain the following items of information:

a. Critical assets that must maintain operations during CBRNE events to support execution of essential missions and functions.

b. CBRNE vulnerabilities to each critical asset.

c. Actions required for remediation of vulnerabilities to each critical asset.

d. Remediation Actions undertaken to eliminate vulnerabilities to each critical asset.

e. CBRNE emergency response plans for each installation and base.

f. All CBRNE Vulnerability Assessments conducted at each installation.

g. Lessons learned from CBRNE emergency response training and exercises.

APPENDIX A

CBRNE PREPAREDNESS AND RESPONSE METRICS

1. Commanders develop, maintain, sustain and assess measures that encourage CBRNE response preparation and effects mitigation. Preparation must be proactive in nature and utilize the four principles; Sense, Shape, Shield, and Sustain, to ensure the safety of all DOD personnel and equipment during a CBRNE incident. Below is a basic checklist that lists the key elements for establishing a comprehensive installation CBRNE protection program:

Yes	No		Reference	Remarks
		Designate a commissioned officer, non-commissioned officer, or a civilian staff officer in writing as the installation CBRNE protection officer with CBRNE emergency response program management responsibilities.	DODI 2000.18	
		Categorize all installations to ensure that each installation understands the requirements for CBRNE protection outline in this Order.	DODI 2000.18	
		Report any initiation of any incident response plan through the proper chain of command via the OPREP-3 reporting requirements.	DODI 2000.18 MARFORNORTH AT OPORD	
		All commands will ensure that realistic CBRNE training and exercises are IAW the NIMS & NRP and are	DODI 2000.18	

		conducted annually. All detailed records of these events shall be maintained per reference (l) SSIC 3005.3.		
		Ensure CBRNE is addressed in all appropriate operational plans, policies, and orders to ensure Installation/facilities CBRNE preparedness capabilities are implemented.	DODI 2000.18	
		Ensure that Supporting Establishment Commands, installations, and facilities, develop and maintain guidance for terrorist incident response and consequence management, to ensure that subordinate commanders will have detail guidance to respond and mitigate to a terrorist incidents if applicable.	DODI 2000.16 DOD O 2000-12H	
		Create and conduct a CBRNE emergency response working groups within each installation to have oversight on planning, assessing, training, and exercising the installation CBRNE program.	DODI 2000.18	
		Invite and include liaison personnel from the appropriate Local,	DODI 2000.18	

		State, and Federal responder community to be attendees of the CBRNE working group.		
		Establish relationships with appropriate local, state, and federal emergency responders to develop a process for creating and implementing MOAs, MOUs with these authorities.	DODI 2000.18	

2. In accordance with the CONOPS the following standards and metric are identified.

CONOPS Reference	Standard	Metric
	With Service support, installation commanders shall equip, train, and exercise personnel appropriately to accomplish integrated installation CBRNE protection	Annually
	Installation CBRNE Preparedness and Response capabilities reviewed for adequacy (includes mutual support memorandums, as appropriate)	Annually
	Identify critical, essential and other DOD/USMC missions and critical assets and infrastructure on installations and facilities	Annually
	Installations assign CBRNE Protection Officer	Annually
	Installations will conduct integrated AT/CBRNE Preparedness and Incident Response exercises in conjunction with local authorities	Annually
	CBRNE Threat information collected IAW DODI 2000.16	Continuously
	CBRNE threat information flow	Annually

CONOPS Reference	Standard	Metric
	procedures are IAW DODI 2000.16	
	Complete Installation CBRNE Protection Risk Assessments	Annually
	Conduct internal integrated vulnerability assessment to include incident management to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies.	Annually
	Incident management subject matter experts (i.e., SMEs who prevent, prepare for, respond to, and recover from CBRNE Events) shall supplement AT/CIP/personnel to assess CBRNE installation vulnerability	Annually
	Comprehensive CBRNE Preparedness and Response planning is integrated in the installation AT plan IAW DODI 2000.16	Annually
	CBRNE Preparedness and Response Planning includes planning for appropriate levels of CBRNE protection for persons who work or live on DOD installations	Annually
	Personnel deemed essential to perform critical DOD/USMC missions (i.e., military, civilian, contractor, host nation, or third-country nationals) are identified, trained, and provided an appropriate level of protection to support mission continuity	Annually
	Integrated CBRNE incident management actions are in place	Annually
	Appropriate mutual aid	Annually

CONOPS Reference	Standard	Metric
	agreements (host nation agreements, etc.) for emergency response are signed	
	Mass CBRNE casualty procedures exist	Annually
	Points of contact for civilian counterpart functions are available in each emergency operations control center	Annually
	Public affairs centers have identified points of contact, emergency protocols, and media expectations	Annually
	Procedures to coordinate and support lead federal agencies following a CBRNE incident are available	Annually
	Procedures exist to determine the extent of CBRNE hazards	Annually
	Procedures exist to collect samples IAW established sampling protocols	Annually
	Be capable of rapidly notifying all appropriate personnel on an installation of CBRNE hazards [Note: Outside CONUS, this includes sponsored dependents living off-site.]	5 Minutes
	Be capable of activating appropriate medical responses (e.g., prophylaxis, vaccines, diagnosis, treatment, etc.) to a CBRNE terrorist incident	15 Minutes
	Action plans are in place to sustain critical mission operations	Yes
	Action plans are in place to recover essential operations from a CBRNE incident	Yes
	CBRNE preparedness and response plan exercised	Annually
	Exercise lessons learned - document and retain	Annually

CONOPS Reference	Standard	Metric
	AT training contains integrated CBRNE protection training. AT training is provided and documented IAW DODI 2000.16	Annually
	Emergency Responder training provided and documented IAW DODI 2000.18	Annually
	Installations use appropriate CBRNE protection construction standards	Yes
	Site selection criteria has been modified to include CBRNE protection concerns	Yes
	Procedures for mail handling include CBRNE protection concerns	Yes
	Tactics, techniques, and procedures exist to sense, shape, shield, and sustain CBRNE incidents	Annually
	Be prepared to preserve CBRNE evidence, collect samples, and implement sample chain of custody rules.	Annually
	Procedures exist to suppress residual CBRNE hazards while protecting evidence	Annually
	Procedures to transition installation CBRNE incident control to federal control and then back to DOD for long-term restoration and recovery	Annually
	Identify potential disposal sites for hazardous waste generated by a potential CBRNE incident	Annually
	Procedures exist to handle contaminated casualties (psychological, injured, or fatalities) at a CBRNE incident site and at military medical facilities	Annually

APPENDIX B

TEMPLATE FOR APPENDIX TO ANNEX C OPORD

APPENDIX 9 TO ANNEX C TO ANTITERRORISM OPORD XX-XXX (U) INSTALLATION CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR AND HIGH-YIELD EXPLOSIVES (CBRNE) PROTECTION (U)

(U) References: See master reference list in Base Order.

1. (U) Situation. Base Order.

a. (U) Purpose. The responsibility to integrate CBRNE training, exercises, and plans into overarching AT plans is critical for synchronized operations. Installation commanders' responsibility is to establish the process to ensure policy and plans are developed that focus installation CBRNE protection, to include interface with local civilian communities. DOD will provide "all personnel at installations and facilities with CBRNE protection, based on appropriate procedures, equipment and training" including military personnel, DOD civilians, contractors, and host nation or third country nationals who work or live on DOD installations and facilities.

2. (U) Mission. Base Order.

3. (U) Execution.

a. (U) Concept of Operation.

(1) (U) All DOD Elements within the AOR will implement a comprehensive Installation CBRNE Protection program. As it may be impossible to determine if a CBRNE release was an accident or a deliberate incident, the installation CBRNE protection program must include an all-hazards approach.

(2) (U) The primary end state is: Protect Personnel, Maintain Installation Critical Missions, and Restore Essential Installation Functions.

(3) (U) Installation CBRNE protection will be accomplished through a tiered installation protection strategy, utilizing four Principles of Passive Defense: Sense, Shape, Shield, and Sustain. Minimum standards are delineated within each Principle by Installation Category. Installations with sufficient resources may exceed Installation Category minimum

standards. Details regarding installation categories and capabilities are shown in the Planning Considerations.

(4) (U) Installations/facilities who cannot meet required capabilities will coordinate for those capabilities with Local, State, Federal authorities or adjacent installations.

(5) (U) All DOD installations in the AOR will adopt and implement the National Incident Management System (NIMS) and the Incident Command System (ICS) as outlined in the National Response Plan (Dec 04). Adoption of appropriate procedures that are consistent with the NIMS and ICS structure will insure that DOD installations in the AOR are functionally aligned to provide or receive emergency response support from State and local first responders.

(6) (U) CBRNE Planning Considerations.

(a) (U) Threat. Terrorist may try to destroy, disrupt or exploit key U.S. military capabilities. Threats include:

1. (U) Chemical. Terrorists may exploit a myriad of toxic industrial chemicals (TICs) available in all parts of the world. These substances are not likely to create as many actual casualties as warfare-strength agents, but are still lethal or highly toxic. Chemical agents can be dispersed using mortars, sprayers, and improvised explosive devices. Chemical effects can last from minutes to weeks at the site of release and create a larger initial hazard area than conventional explosives. Further, chemicals often create a temporary downwind vapor hazard.

2. (U) Biological. Biological hazards pose unique challenges because they are relatively easy to produce and difficult to detect after release. Examples of terrorist biological weapons include small amounts of anthrax or smallpox dispersed using a non-explosive point source or spray tank. The duration of agent virulence and the size of the downwind hazard area are largely dependent on environmental conditions and dissemination efficiency at the time of the attack. The potential psychological impact and relative low cost of biological hazards make them an attractive alternative to explosives. Offensive biological programs can be easily concealed, and production does not always require specialized equipment. Effective medical intervention is possible for many

bacteria, but other pathogens (e.g., viruses, fungi, toxins) can be much more difficult to treat.

3. (U) Radiological. Low-level radiological material is available from a large number of industrial sources worldwide. Terrorists able to gain access to this material could exploit it using low-yield explosive devices. Specific examples of terrorist radiological hazards include iridium, cesium, and highly enriched uranium (HEU) as the core of a radiological dispersal device. Although rarely lethal in the near term, the deliberate dissemination of radioactive matter can cause considerable immediate psychological harm and require enormous remediation/restoration operations.

4. (U) Nuclear. Terrorists with sufficient finances may seek out those willing to sell both information and materiel regarding nuclear weapons. Besides the extremely high explosive nature of nuclear weapons, other effects include high-altitude electromagnetic pulse (HEMP/EMP) that may degrade unprotected and vulnerable military and civilian devices.

5. (U) Explosive. Virtually every country, sub-national group, and terrorist organization has access to explosive devices. Traditionally, these have been the weapons of choice to terrorists because they are readily available, cheap, easy to use, and their effects are reasonably predictable. Although there is considerable psychological impact with terrorist use of an explosive device, most actual casualties are created in the immediate area of the blast.

(7) (U) Installations will utilize the Sense, Shape, Shield, and Sustain (4S) construct (as outlined in ref. ff) for CBRNE Preparedness. However, the AT community uses slightly different terms to discuss their preparedness capabilities. The AT community uses Detect and Assess (as opposed to Sense); Report (as opposed to Shape); Prevent/Deter and Defend (as opposed to Shield); and Recover (as opposed to Sustain). Figure C-9-1 is an overlay depicting how the four principles for Installation CBRNE Protection and the Antiterrorism principles parallel each other:

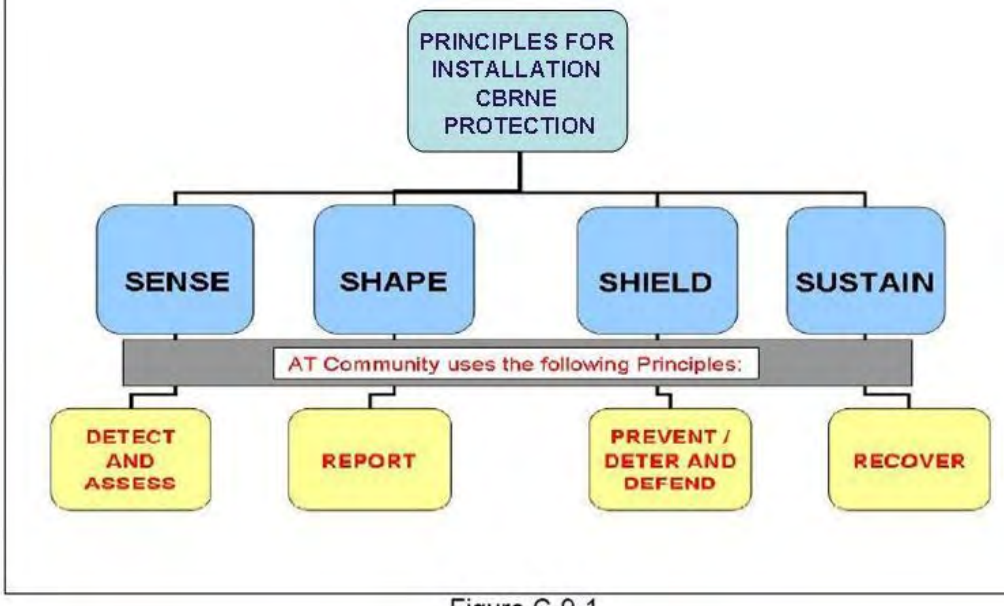


Figure C-9-1

The tiered protection strategy matching installation classes and required/desired 4S capabilities are shown in Table C-9-2.

UNCLASSIFIED/
FOR OFFICIAL USE ONLY

Installation Classes	CLASS 1	CLASS 2	CLASS 3	CLASS 4	CLASS 5
Capabilities					
Sense 1	Desired				
Sense 2	Required	Required	Desired		
Shape	Required	Required	Required	Required	
Shield 1	Required	Required	Required	Required	Required
Shield 2	Required	Required			
Sustain	Provided by external Federal, State, and local Agencies (and host nation as applicable)				

Table: C-9-2

(a) (U) Sense: The ability to maintain awareness of the current CBRNE situation by detecting and identifying CBRNE hazards in the air, water, food, or soil; on personnel, equipment or facilities; and, determining the physical state of those hazards (solid, liquid, gaseous). This principle includes the capability to quantify and sample CBRNE hazards. Sense is the key enabler, using knowledge-based human and state-of-the-art detection equipment, for shaping the commander's understanding of the hazard. SENSE categories are as follows:

1. (U) Sense 1, Stand-off Detection and Reconnaissance.

a. (U) Stand-off detectors can increase the effectiveness of early warning of CBRNE hazards and assess large areas for potential contamination, thus allowing the commander to make rapid decisions on active defense, evacuation, shelter-in-place, and other protective measures. The employment of these sensors calls for careful placement to provide adequate coverage, and often can require specialists to operate.

b. (U) Reconnaissance. If an installation or facility lacks the ability to perform stand-off or automated point detection, it may fall to dedicated CBRNE specialists or installation emergency responders to reconnoiter the hazard area with specialized equipment as the incident unfolds.

2. (U) Sense 2, Automatic Point Detection and Medical Surveillance.

a. (U) Automatic and manual point detectors offer installation personnel tools to detect, identify, quantify, and sample CBRNE hazards to provide decision makers with critical information. Since point detectors by their nature only inform personnel in the immediate vicinity of potential hazards, it is crucial that these detectors be emplaced at critical sites on the installation and networked into the emergency operations center. If the use of automatic detectors at critical sites is not a feasible option, the commander may need to utilize emergency responders with appropriate manual detectors and communications equipment. The intent is not to necessarily employ 24/7 monitoring capability but rather to allow automatic detection and identification capability in times of increased threat conditions.

b. (U) Medical surveillance. Although medical surveillance is a broad area supporting Force Health Protection (FHP) in general, the reporting of non-battle disease injuries is a critical function. Combined with the local civilian health surveillance and worker absentee data, the medical specialists should note and report trends in health that may be indicative of a Biological Warfare (BW) terrorist attack.

(b) (U) Shape: The ability to provide the capability to characterize the CBRNE hazard for the commander. CBRNE hazard characterization is the process by which the commander develops a clear understanding of the current and predicted CBRNE hazard situation, envisions critical mission end states, and develops the sequence of events that moves the installation from its current state to those end states. By manually and automatically collecting and assimilating CBRNE hazard information from civilians, military personnel, host nation (as applicable), and Local/State/Federal response assets in near real time, the commander is able to observe actual and potential effects of CBRNE hazards and to make timely decisions. SHAPING categories consist of:

1. (U) Decision Support Tools. Utilize existing/ future command and control systems and resources to ensure accurate assessment and dissemination of CBRNE hazards to the installation population and with military, local, State and Federal emergency operations centers. Installation command centers require CBRNE Preparedness decision support tools that access and assimilate CBRNE hazard data from throughout the installation. Hazard prediction tools must reside with command and control equipment that is ideally interfaced with automated sensors on an installation. In addition, these tools must include the ability to input meteorological, medical, and terrain data that influences the CBRNE hazard effects on a near-real time basis as well as for predictive analysis, allowing the commander to determine the risk associated with various courses of action.

2. (U) Mass Alert Notification. Installations and facilities must have the capability to notify, within 10 minutes, all personnel on an installation/facility, as well as affected military personnel and dependents off-site, of an impending or actual CBRNE hazard incident. Signals and notifications must be clear and unambiguous to avoid confusion. Additionally, installations and facilities must ensure that their notification procedures include specific steps to pass

alerts to local/regional response systems in order to alert surrounding communities to hazards.

(c) (U) Shield: The commander, or civilian equivalent, shields his/her personnel by providing appropriate levels of physical protection, training and medical pre-treatment, to the extent possible. The commander relies on First Responders as the second tier of shielding installation personnel. This is accomplished through the rapid response, assessment, and initial recovery operations undertaken to safeguard personnel from continued hazards, to control contamination, and to initiate steps to restore the area to its pre-incident conditions.

1. (U) Shield 1. Mission essential personnel protection will be provided the appropriate level of protection necessary to support mission continuity for up to 12 hours. Non-mission essential personnel protection will be provided protection and/or procedures necessary to survive an incident safely. Plans and procedures will address evacuation, shelter in place, and/or the issue/use of personal protective equipment. The goal is to have 90 percent of the installation/facility (DOD-leased, -owned, or -managed) initiating evacuation or shelter-in-place measures within 15 minutes of incident notification.

2. (U) Shield 2. Installation/facility emergency responders are responsible for assessing the hazard and saving lives. Installation/facility emergency response equipment must meet National Institute for Occupational Safety and Health (NIOSH), National Fire Protection Association (NFPA), , and all other applicable standards that address operations in CBRNE hazard environments. Emergency medical technicians and hospitals will require medical diagnosis tools and medical countermeasures for CBRNE hazards. Commanders should consider off-installation response capabilities as well as on-installation. Minimum first responder capabilities (for those organizations that have organic first responder capabilities) are outlined in Tab B. Those installations that have limited or no first responder capability must ensure that they are integrated into the host installation or local community first responder notification and response plans.

(d) (U) Sustain: Sustaining critical operations during a CBRNE incident and resuming essential operations following a CBRNE event will require additional capabilities in order to promptly revert to pre-incident operational

capability/readiness. Mission recovery and sustainment are undertaken concurrent with or subsequent to initial response actions to restore or sustain mission operational capability. Sustain consists of dedicated DOD organizations/units and civilian response agencies organized, equipped, and trained to decontaminate and treat personnel, equipment, and critical infrastructure facilities to regain their full capability as quickly as possible. In most situations, commanders will not be able to maintain and sustain an inherent capability to continue long-term recovery and restoration efforts and return the installation to pre-incident conditions. Installations should identify and determine the capabilities of their applicable civilian response agencies that may be available should a CBRNE incident occurs. The successful completion of this task will require prior planning and agreements with local, State, and Federal emergency response agencies.

b. (U) Tasks.

(1) (U) Installation commanders will:

(a) (U) Exercise overall responsibility to protect, prevent loss or mitigate loss of personnel, critical missions, and assets on DOD installations or facilities within the AOR under the authority of TACON for FP.

(b) (U) Coordinate with the DOD Elements to categorize all installations and facilities IAW Tab A (Installation Classes) in order to determine the appropriate CBRNE preparedness level.

(c) (U) Ensure information/intelligence requirements address CBRNE specific issues.

(d) (U) Develop a process that rapidly determines if a CBRNE threat is directed towards an installation or facility.

(e) (U) Coordinate and partner with DOD and non-DOD agencies regarding CBRNE preparedness.

(f) (U) Ensure CBRNE is addressed in all plans, orders and exercises. Review and provide input to higher headquarters CBRNE policy.

(g) (U) Establish CBRNE assessment standards/ benchmarks. Incorporate CBRNE standards in NC program reviews and vulnerability assessment program IAW Annex C.

(h) (U) Identify, document, validate, prioritize and submit to the Joint Staff resource requirements necessary to ensure installation CBRNE preparedness. This process is addressed in Appendix 7, paragraphs b.(3) thru (10), pages C-7-4 thru C-7-9.

(i) (U) Develop CBRNE remediation and risk mitigation measures for the protection of installations/facilities and maintain a database of those measures.

(j) (U) Ensure CBRNE warning and reporting requirements are addressed in information architecture requirements and development.

(k) (U) Perform HHQ vulnerability assessments/ security assessments triennially IAW CBRNE/Contingency Operations VA, format TBD. Report results of VA on CVAMP or similar IT architecture IAW the reporting requirements directed in Appendix 6 to Annex C and Annex R of this OPORD.

(2) (U) Develop appropriate plan to respond to CBRNE events on installations within the AOR.

(3) (U) Elements will:

(a) (U) DOD Elements within the AOR will implement a comprehensive Installation CBRNE Protection program as outlined in paragraph 3 of this Appendix. Training and Exercise requirements are outlined in Tab C (Installation CBRNE Protection Training and Exercises).

(b) (U) Pass information and intelligence regarding CBRNE through existing information/intelligence reporting channels/requirements outlined in Annex C, Appendix 1.

(c) (U) Coordinate and partner with Federal, State and Local authorities regarding installation CBRNE protection.

(d) (U) Address CBRNE in all operational plans, orders and exercises to ensure installation CBRNE preparedness capabilities are maintained.

(e) (U) Classify their installations and facilities in order to determine the appropriate CBRNE preparedness level.

Provide a list of their installations by class IAW Tab A NLT x Oct 07.

(f) (U) Develop AT and Physical Security Plans that integrate facilities, equipment, personnel and procedures to maximize CBRNE protection.

(g) (U) Provide remediation and mitigation of CBRNE vulnerabilities for installations and facilities.

(h) (U) Ensure annual vulnerability assessment or security assessment as appropriate on all installations and facilities are conducted. All assessments will be provided to the NC/J34 Assessments Branch and loaded in CVAMP. Installation commanders will establish CBRNE assessment standards at a date TBD.

(i) (U) Identify, document, validate, prioritize and submit resource requirements necessary to ensure the installation CBRNE preparedness. PPBE submissions and CbT RIF are outlined in Annex C, Appendix 7.

(j) (U) Report initiation of any CBRNE incident response plan through the proper chain of command IAW Appendix 1, paragraph b.(1)(h) Crisis Reporting. Notification will include the NORAD-XXXXXXXXXX Command Center.

(k) (U) Consider the establishment of a CBRNE Preparedness Officer at the installation level to work in conjunction with the AT Officer/staff.

(l) (U) Establish clear command, control, and communication lines between local, State, Federal, and Host Nation emergency assistance agencies that detail support relationships and responsibilities.

(m) (U) Address Top 3 CBRNE issues in DOD Element Monthly FP Readiness and Update. Annex R, Reports.

(n) (U) Provide installations with:

1. (U) Tasking POCs for their CBRNE program offices.

2. (U) 24-hour operations center contact information, or 24-hour POC if no operations center is available.

3. (U) Information necessary for XX/XXX to establish accounts/passwords for access to the website/restricted portal.

4. (U) Ensure all information is current and updated on a monthly basis.

(o) (U) Ensure that the Medical Response and IM Program are integrated into the Command's FP Program.

Tabs:

A. Installation Classes (U)

B. First Responder Minimum Requirements (U)

C. Installation CBRNE Preparedness Training and Exercises (U)

APPENDIX C

FORMAT FOR AN OPREP-3SIR MESSAGE

FROM: MCB CAMP LEJEUNE
TO: CMC WASHINGTON DC//POC//
INFO: CMC WASHINGTON DC//PS//
(CLASS) //N05740//
EXER/EXERCISE NAME/ADDITIONAL IDENTIFIER//
EXERCISE NAME = ENTER THE EXERCISE NAME
ADDITIONAL IDENTIFIER = ENTER THE ADDITIONAL EXERCISE IDENTIFIER
(DO NOT USE EXER AND OPER IN THE SAME MESSAGE)
OPER/OPERATION NAME/PLAN ORIGINATOR/OPTION NAME/2D OPTION NAME//
OPERATION NAME = SELF EXPLANATORY
PLAN ORIGINATOR = PLAN ORIGINATOR AND NUMBER
OPTION NAME = CODE NAME FOR OPERATIONS WITHIN THE OPERATION PLAN
2D OPTION NAME = SECOND CODE NAME FOR OPERATION WITHIN THE
OPERATION PLAN

MSGID/TITLE/UNIT/SERIAL #/MONTH/QUALIFIER/QUALIFIER SERIAL #//
TITLE= OPREP-3 SIR
UNIT= UNIT ORIGINATING MSG
SERIAL # = FIRST INCIDENT REPORTED EACH CALENDAR YEAR WILL BE
SERIAL
001. ALPHABETIC SUFFIX (E.G., 001A, 001B, ETC.) WILL IDENTIFY
ADDITIONAL REPORTS ON THE SAME INCIDENT. REPORTS OF SUBSEQUENT
INCIDENTS WILL BE SERIALIZED NUMERICALLY (I.E: 002 THROUGH 999).
MONTH= FIRST THREE LETTERS OF THE MONTH
QUALIFIER= IF THIS IS A FIRST REPORT THIS FIELD IS BLANK; IF
THIS MSG PROVIDES ADDITIONAL INFORMATION USE AMP FOR AMPLIFIES
OR DEV FOR DEVIATIONS FROM A PREVIOUS MESSAGE.
QUALIFIER SERIAL = HOW MANY MESSAGES HAVE BEEN SENT QUALIFYING
THE BASIC MESSAGE: THE INITIAL VOICE REPORT DOES NOT COUNT AS A
MESSAGE TO BE AMPLIFIED.)

REF/SERIAL LETTER/ORIGINATOR/DTG/SERIAL #/SPECIAL NOTATION//
SERIAL LETTER = (USMTF MESSAGE SHORT TITLE) OR (TYPE OF
REFERENCE = DOC
FOR DOCUMENT, TEL FOR TELEPHONIC NOTIFICATION, MSG FOR MESSAGE)
ORIGINATOR = SELF EXPLANATORY
DTG = DATE TIME GROUP
SERIAL NUMBER = REFERENCED MSG
SPECIAL NOTATION = NOTAL OR PASEP FOR REFERENCES NOT SENT TO ALL
MSG ADDRESSEES, OR TO BE PASSED SEPARATELY)

NARR/FREE TEXT TO EXPLAIN REFERENCES//
FLAGWORD/PRIMARY FLAGWORD/SECONDARY FLAGWORD//

PRIMARY FLAGWORD = ENTER /-/
SECONDARY FLAGWORD = ENTER /SERIOUS INCIDENT REPORT//

TIMELOC/DTG/LOCATION/REPORT STATUS//
DTG = ZULU DTG OF INCIDENT
LOCATION = LOCATION OF INCIDENT OR UNIT AT TIME OF INCIDENT
REPORT STATUS = (INIT=INITIAL, FOLUP=FOLLOWUP, CORR=CORRECTION, OR FINAL)//

GENTEXT/INCIDENT IDENTIFICATION AND DETAILS/1. SUMMARIZE FACTUAL INFORMATIONCONCERNING THE INCIDENT. THE EXTENT OF INJURIES TO PERSONNEL AND ESTIMATED DOLLAR VALUE OF DAMAGES OR LOSS WILL BE INCLUDED. REPORT THE EXACT LOCATION USING THE NAME OF THE LOCATION OR MILES TO THE NEAREST IDENTIFIABLE LANDMARK.USE MAP GRID COORDINATES ONLY WHEN OTHER MEANS OF IDENTIFYING THE LOCATION ARE IMPRACTICABLE, AND THEN IDENTIFY THE MAP COMPLETELY.

2. POINT OF CONTACT: CONTACT NAME, MILITARY RANK, PHONE NUMBERS, BILLET.

3. PERSONNEL INVOLVED:

A. SUSPECT, VICTIM, WITNESS, SENTRY, DRIVER, OR OTHER APPROPRIATE
DESCRIPTION
(1) GRADE OR TITLE.
(2) FIRST NAME, MIDDLE INITIAL, LAST NAME.
(3) SOCIAL SECURITY NUMBER (SSN). (IF CIVILIANS, INDICATE THEIR STATUS; IE., DEPENDENT, ETC., IN PLACE OF SSN.)
(4) UNIT ORGANIZATION OR ADDRESS.
(5) RACE, SEX: (E.G., AMER-INDIAN, FEMALE) RACE OPTIONS SEX AMER-INDIAN / ALASKAN NATIVE MALE ASIAN / PACIFIC ISLANDER FEMALE BLACK WHITE UNKNOWN AMPLIFY RACE DETAILS AS NEEDED IN THE GENTEXT.
(6) STATUS (I.E., HOSPITALIZED) AND LOCATION OF PERSONNEL INVOLVED.

B. REPEAT PARAGRAPH A FOR ADDITIONAL SUSPECTS, VICTIMS, WITNESSES OR OTHERS AS NECESSARY.

4. DESIGNATION OF THE ORGANIZATION OR OFFICES, MILITARY AND CIVILIAN, CONDUCTING THE INVESTIGATION OR POINT OF CONTACT FOR ADDITIONAL INFORMATION.

5. STATEMENT AS TO PRESENT OR ANTICIPATED REACTION OF THE CIVIL POPULACE TO THE INCIDENT. INCLUDE A STATEMENT THAT THE COGNIZANT

PUBLIC AFFAIRS OFFICE (HAS) (HAS NOT) BEEN NOTIFIED OF THIS INCIDENT. INCLUDE PRESENT MEDIA COVERAGE TO DATE AND ANTICIPATED NEWS MEDIA INTEREST IN THE INCIDENT.

6. STATEMENT THAT THE LOCAL INTELLIGENCE OFFICER (HAS) (HAS NOT) BEEN NOTIFIED OF THIS INCIDENT.

7. FURTHER ACTION BEING TAKEN.
DECL/ENTER DECLASSIFICATION OR DOWNGRADING INSTRUCTIONS//

APPENDIX D

DEFINITIONS

1. Antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

2. Biological Agent. A microorganism that causes disease in personnel, plants, or animals or causes the deterioration of materiel.

3. Chemical Agent. Any toxic chemical intended for use in military operations.

4. Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Incidents. An emergency resulting from the deliberate or unintentional release of nuclear, biological, radiological, or toxic or poisonous chemical materials, or the detonation of a high-yield explosive. Also called CBRNE incidents.

5. Combating Terrorism. Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counter-terrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum.

6. Consequence Management. Actions taken to maintain or restore essential services and manage and mitigate problems resulting from disasters and catastrophes, including natural, manmade, or terrorist incidents. Also called CM.

7. Crisis Management. Measures to identify, acquire, and plan, the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism. Crisis Management is predominantly a law enforcement response, normally executed under federal law.

8. Domestic Emergencies. Emergencies affecting the public welfare and occurring within the 50 States, District of Columbia, Commonwealth of Puerto Rico, U.S. possessions and territories, or any political subdivision thereof, as a result of enemy attack, insurrection, civil disturbance, earthquake, fire, flood, or other public disasters or equivalent emergencies that endanger life and property or disrupt the usual process of

government. The term domestic emergency includes all of the emergency conditions defined below:

a. Civil Defense Emergency. A domestic emergency disaster situation resulting from devastation created by an enemy attack and requiring emergency operations during and following the attack. It may be proclaimed by appropriate authority in anticipation of an attack.

b. Civil Disturbances. Riots, acts of violence, insurrections, unlawful obstructions or assemblages, or other disorders prejudicial to public law and order. The term "civil disturbance" includes all domestic conditions requiring or likely to require the use of Federal Armed Forces pursuant to the provisions of 10 USC Chapter 15.

c. Major Disaster. Any flood, fire, hurricane, tornado, earthquake, or other catastrophe which, in the determination of the President, is or threatens to be of sufficient severity and magnitude to warrant disaster assistance by the Federal Government under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 USC 5121, et seq) to supplement the efforts and available resources of State and local governments in alleviating the damage, hardship, or suffering caused thereby.

d. Natural Disaster. All domestic emergencies except those created as a result of enemy attack or civil disturbance.

9. Emergency Responders. Firefighters, law enforcement/ security personnel, and emergency medical technicians, emergency management and operations personnel, Explosive Ordnance Disposal (EOD) personnel, physicians, nurses, medical treatment providers at medical treatment facilities, disaster preparedness officers, public health officers, bio-environmental engineers, and mortuary affairs personnel.

10. First Responders. Firefighters, law enforcement and/or security personnel, emergency medical technicians, and EOD personnel (for suspected explosive CBRNE events) that provide the initial, immediate response to a CBRNE incident.

11. Force Protection. Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. Force protection does not include actions to

defeat the enemy or protect against accidents, weather, or disease. Also called FP.

12. Foreign Consequence Management. Assistance provided by the United States Government to a host nation to mitigate the effects of a deliberate or inadvertent chemical, biological, radiological, nuclear, or high-yield explosives attack or event and restore essential government services. Also called FCM.

13. High-Yield Explosive. Any conventional weapon or device that is capable of a high order of destruction or disruption and/or of being used in such a manner as to kill or injure large numbers of people. (HYE is the 'E' in CBRNE).

14. Installation. A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

15. Installation Commander. The individual responsible for all operations performed by an installation.

16. Immediate Response. Any form of immediate action taken to assist civil authorities or the public to save lives, prevent human suffering, or mitigate great property damage under imminently serious conditions when time does not permit approval from a higher authority.

17. Lead Agency. Designated among US Government agencies to coordinate the interagency oversight of the day-to-day conduct of an ongoing operation. The lead agency is to chair the interagency working group established to coordinate policy related to a particular operation. The lead agency determines the agenda, ensures cohesion among the agencies, and is responsible for implementing decisions.

18. Lead Federal Agency. The federal agency that leads and coordinates the overall federal response to an emergency. Designation and responsibilities of a LFA vary according to the type of emergency and the agency's statutory authorities. The Federal Bureau of Investigation is the LFA for all crisis management, foreign or domestic. Federal Emergency Management Agency is the LFA for domestic consequence management and the Department of State is the LFA for foreign consequence management.

19. Mutual Aid Agreement (MAA). Reciprocal assistance by local

government and an installation for emergency services under a prearranged plan. Mutual aid is synonymous with "mutual assistance," "outside aid," "memorandums of understanding," memorandums of agreement, "letters of agreement," "cooperative assistant agreement," "intergovernmental compacts," or other similar agreements, written or verbal, that constitute an agreed reciprocal assistance plan for emergency services for sharing purposes. MAAs between entities are an effective means to obtain resources and should be developed whenever possible. MAAs should be in writing, be reviewed by legal counsel, and be signed by a responsible official.

20. National Disaster Medical System. A coordinated partnership between Departments of Homeland Security, Health and Human Services, Defense, and Veterans Affairs established for the purpose of responding to the needs of victims of a public health emergency. Also called NDMS.

21. Terrorism. The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

22. Terrorist Emergency Response Measures. Procedures in place on a DOD installation for emergency response forces to deal with the effects of a CBRNE incident.

23. Vulnerability. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.

24. Vulnerability Assessment. A DOD, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. Also called VA.

25. Weapons of Mass Destruction. Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. WMD can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. Also called WMD.

26. Weapons of Mass Destruction - Civil Support Team.(WMD-CST). WMD-CSTs are comprised of both Army and Air National Guard personnel. They are Federally funded and equipped to provide State governors ready access to fully trained military CM response assets to use in preparing for and responding to WMD incidents as part of their State emergency management response system. Additionally, they provide the Department of Defense's unique expertise and capabilities to complement and enhance the State and local civil authorities' response capabilities. Also called WMD-CST.

APPENDIX E

ADDITIONAL RESOURCES

1. Deputy Secretary of Defense Memorandum, “Preparedness of U.S. Military Installations and Facilities Worldwide Against Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Attack,” September 5, 2002

2. Deputy Secretary of Defense Memorandum, “Response to Program Decision Memorandum III (PDM III), CBRNE Installation Protection Action Plan,” May 8, 2007

3. Department of the Navy Consequence Management Planning Guide

4. Joint Publication 3-11, “Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments,” July 11, 2000

5. DOD Directive 2000.12, “DOD Antiterrorism (AT) Program,” August 18, 2003

6. CJCSI 3435.01, “Standards for Chemical, Biological, Radiological, Nuclear, and High Yield Explosive (CBRNE) Protection on Installations and Facilities,” June 8, 2004

7. 9230.1-PL, “Federal Response Plan-Interim,” Federal Emergency Management Agency, April 1999

8. DOD Protection Joint Functional Concept, Version 1, December 31, 2003

9. DOD Directive 3025.1, “Military Support to Civil Authorities (MSCA),” January 15, 1993

10. DOD Directive 3025.15, “Military Assistance to Civil Authorities,” February 18, 1997

11. DOD O-2000.12-H, “DOD Antiterrorism Handbook,” February 1, 2004

12. DOD Critical Infrastructure Protection (CIP) Plan, November 18, 1998

13. DOD CIP Strategy, April 2003

14. DOD Directive 3020.40, “Defense Critical Infrastructure Program (DCIP),” August 19 2005

15. Homeland Security Presidential Directive (HSPD) #7, “Critical Infrastructure Identification, Prioritization, and Protection,” December 17, 2003

16. “Initial National Response Plan,” U.S. Department of Homeland Security, September 30, 2003

17. DOD Directive 1404.10, “Emergency Essential (EE) DOD U.S. Citizen Civilian Employees,” April 10, 1992

18. DOD Instruction 1400.32, “DOD Civilian Workforce Contingency and Emergency Planning Guidelines and Procedures,” April 24 1995

19. 9230.1-PL , “Federal Response Plan (FRP)-Interim,” Federal Emergency Management Agency, December 2004

20. U.S. Department of Homeland Security, “National Incident Management System (NIMS),” March 1, 2004

21. Homeland Security Presidential Directive/HSPD-5, “Management of Domestic Incidents,” February 28, 2003

22. Homeland Security Presidential Directive/HSPD-7, “Critical Infrastructure Identification, Prioritization, and Protection,” December 17, 2003

23. Homeland Security Presidential Security Directive/HSPD-8, “National Preparedness,” December 17, 2003

24. Unified Facilities Criteria 4-010-01, “DOD Minimum Antiterrorism Standards for Buildings,” July 31, 2002

25. Joint Publication 4-06, “Mortuary Affairs in Joint Operations,” June 5, 2006